

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-214283

(43)公開日 平成8年(1996)8月20日

(51) Int.Cl.<sup>6</sup>  
H 0 4 N 7/173

識別記号      庁内整理番号      F I

### 技術表示箇所

審査請求 未請求 請求項の数36 OL (全 19 頁)

(21)出願番号 特願平7-17827

(22)出願日 平成7年(1995)2月6日

(31)優先權主張番号 193410

(32)優先日 1994年2月7日

(33)優先権主張国 米国 (US)

(71)出願人 592083122

ル・グループ・ビデオトロン・リミテ  
LE GROUPE VIDEOTRON  
LTEE

カナダ、アッシュ2イクス・3ダブルヴェ4、ケベック、モントリオール、アヴニユー・ヴィガール・エスト300番

(72)発明者 ピエール・ガルノー

カナダ、アッシュ2イグレク・1ゼッド  
5、ケベック、モントリオール、サン・ボ  
ール・ウエスト・ヌメロ32・157番

(74)代理人 弁理士 青山 葆 (外2名)

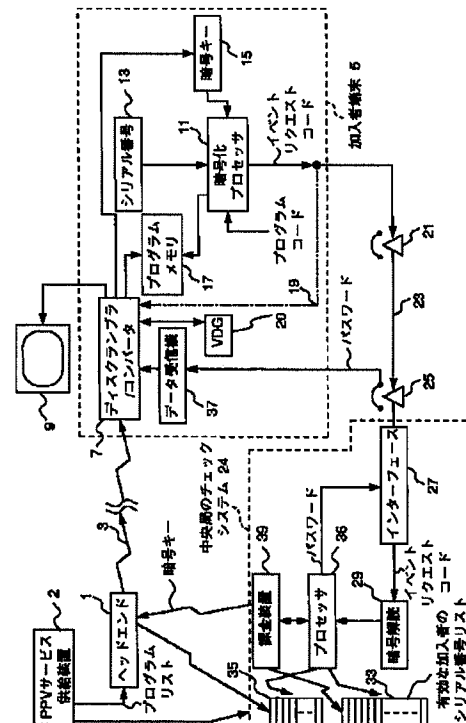
[最終頁に続く](#)

(54) 【発明の名称】 CATVシステムの有効な加入者に信号を分配するための方法及びCATVシステム

(57) 【要約】

**【目的】** ヘッドエンドから端末に対してデスクランブルコードをダウンロードすることを必要とせず、サービス提供者がサービスを提供することを可能にすることができるCATVシステムの有効な加入者に信号を分配するための方法とCATVシステムを提供する。

【構成】 複数のサービスの1つを選択しかつ選択されたサービスの販売促進コードを1つの端末に入力させる。選択された販売促進コードの入力に応答して端末と関連する識別番号を自動的に読み出し、暗号化アルゴリズムに従って識別番号と選択された販売促進コードとを処理して暗号化されたイベント要求コードを発生した後、認証センタに供給し、認証センタはイベント要求コードを暗号解読してパスワードを供給する。パスワードの端末への入力に応答して販売促進コードに対応する複数の信号の1つを利用するサービスに対するアクセスを端末に提供する。



**【特許請求の範囲】**

【請求項1】 複数の信号を有効な複数の加入者に対して分配するための方法であって、(a) 中央局において、有効な複数の加入者端末識別コードを記憶することと、(b) それぞれが特定の販売促進コードと関連する複数の加入者に利用可能な複数のサービスの販売促進を放送することと、(c) 上記複数のサービスの1つを選択しかつ選択されたサービスの販売促進コードを加入者のロケーションにおける1つの端末に入力させることと、(d) 上記選択された販売促進コードの入力に応答して、上記端末と関連する識別番号を自動的に読み出すことと、(e) 暗号化アルゴリズムに従って上記識別番号と上記選択された販売促進コードとを処理し、かつそこから暗号化されたイベント要求コードを発生することと、(f) 上記イベント要求コードを認証センタに供給することと、(g) 上記認証センタにおいて、上記イベント要求コードを暗号解読し、かつ上記端末と上記選択された販売促進コードに唯一であるパスワードを供給することと、(h) 上記パスワードを上記加入者のロケーションにおける端末に入力させることと、(i) 上記パスワードの入力に応答して、上記選択された販売促進コードに対応する分配された複数の信号の1つを利用することとを含むことを特徴とする方法。

【請求項2】 ケーブルネットワークによる上記複数のサービスを上記複数の加入者に分配することを含むことを特徴とする請求項1記載の方法。

【請求項3】 上記識別番号は固定され、上記各端末におけるROMとスイッチの一群のうちの1つに格納されたことを特徴とする請求項1記載の方法。

【請求項4】 上記識別番号は変化可能であり、RAMに格納され、上記各端末と関連する固定されたアドレスをさらに含み、

上記識別番号は、上記固定されたアドレスによって識別された加入者にアドレス指定されたケーブルを介して受信されることを特徴とする請求項2記載の方法。

【請求項5】 上記複数の端末のそれぞれに暗号キーを送信することと、  
上記暗号キーを上記各端末で格納することを含むことを特徴とする請求項2記載の方法。

【請求項6】 上記各端末は固定されたアドレスを有し、  
上記方法は、  
複数の暗号キーを上記固定されたアドレスによって識別された上記複数の端末に送信することと、  
上記各端末で現在の暗号キーを格納することを含むことを特徴とする請求項2記載の方法。

【請求項7】 上記複数の販売促進コードに関する複数のプログラムコードを上記複数の端末のそれぞれに送信することと、

上記販売促進コードとしてのプログラムコードと、端末識別コードとを、格納された暗号キーを用いて暗号解読しかつ符号化して上記イベント要求コードを発生することを含むことを特徴とする請求項5記載の方法。

【請求項8】 上記各固定された識別番号は、上記各端末におけるROMに格納されることを特徴とする請求項6記載の方法。

【請求項9】 上記複数のサービスのうちの少なくとも1つはペイパービューテレビジョン信号であることを特徴とする請求項7記載の方法。

【請求項10】 上記テレビジョン信号はスクランブルされ、上記アクセスを提供するステップは、上記パスワードの入力時に、上記信号をデスクランブルすることを含むことを特徴とする請求項9記載の方法。

【請求項11】 複数の信号を有効な複数の加入者に対して分配するための方法であって、(a) 加入者端末において、サービスに格納されたプログラムコードと、上記端末の識別に関するアドレスコードとをアクセスすることによって、上記複数の信号を利用するサービスのための要求コードを発生し、かつ端末暗号キーを用いて上記複数のコードを暗号化してサービス要求コードを発生することと、(b) 上記サービス要求コードを提供することによって中央端末からの上記サービスを要求することと、(c) 上記中央端末において、上記サービス要求コードを暗号解読し、上記アドレスコードと上記プログラムコードとの有効性をチェックし、かつ1つのパスワードを発生することと、(d) 上記パスワードを上記加入者端末に入力し、上記複数の信号に対するアクセスを提供することに応答して、上記サービスを提供することを含むことを特徴とする方法。

【請求項12】 ヘッドエンドから上記加入者端末に暗号キーをダウンロードすることを含むことを特徴とする請求項11記載の方法。

【請求項13】 ケーブル分配器又は複数のオペレータ暗号キーは、各加入者端末が端末アドレスによって識別された複数の加入者端末にダウンロードされることを特徴とする請求項12記載の方法。

【請求項14】 複数の放送事業者によって上記複数の信号を供給することと、  
同一の暗号キーを各放送事業者に登録されたすべての加入者にダウンロードすることを含み、  
異なった暗号キーが異なった放送事業者に登録された複数の加入者に供給されることを特徴とする請求項13記載の方法。

【請求項15】 上記複数の信号は、すべての上記複数の放送事業者によって共通に使用されたケーブルネットワークを介して分配されることを特徴とする請求項14記載の方法。

【請求項16】 上記要求コードは、加入者に注意するためにテレビジョンのスクリーン上に表示され、上記サ

ービスが要求されることを特徴とする請求項1記載の方法。

【請求項17】 ケーブルテレビジョンシステムであって、  
上記ケーブルテレビジョンシステムは、

(a) 複数の加入者端末を備え、上記各加入者端末は、  
(i) 端末識別コードを格納するための手段と、(ii) プログラム識別コードを格納するための手段と、(iii) 暗号キーを格納するための手段と、(iv) 暗号化アルゴリズムに従って上記複数のコードと上記キーとを処理することにより、プログラム要求コードを発生するための手段と、(v) 複数のプログラムを表示し、かつ上記プログラム要求コードを表示するためのディスプレイと、(vi) 1つのパスワードを受信し、それに応答して通過すべきプログラムを上記ディスプレイ上に表示するために上記ディスプレイに入力するための手段とを備え、

(b) ヘッドエンドと、上記ヘッドエンドに接続されたCATVネットワークとを備え、上記ヘッドエンドは、上記プログラムのスクランブルされた信号を上記CATVネットワークを介して上記複数の加入者端末に送信し、

(c) 中央局を備え、上記中央局は、(i) 上記プログラム要求コードを受信するための手段と、(ii) 上記プログラム要求コードを暗号解読し、そこから上記プログラム識別コードと上記端末識別コードを決定するための手段と、(iii) 上記決定されたプログラムと端末識別コードとの有効性を認証するための手段と、(iv) 上記決定されたプログラムと端末識別コードの有効性の認証に応答して上記パスワードを発生するための手段とを備えたことを特徴とするケーブルテレビジョンシステム。

【請求項18】 上記中央局における上記受信するための手段は、

電話回線に接続され、加入者によって上記電話回線を介して入力された上記プログラム要求コードの各ディジットを検出するための自動タッチトーン信号検出回路と、上記パスワードの音声化された音声信号を合成的に発生し、かつ当該音声信号を上記加入者によって受信するために上記電話回線に印加するための音声応答装置とを備えたことを特徴とする請求項17記載のシステム。

【請求項19】 上記システムは、複数の中央局を備え、

上記各中央局は異なったケーブルテレビジョンのオペレータによって操作され、上記ケーブルテレビジョンのオペレータのすべては、同一のネットワーク上の複数のプログラムを複数の加入者端末の一群に分配し、  
上記複数の加入者端末における複数の暗号キーは、すべて同一である1人のケーブルテレビジョンのオペレータから受信することを許可されるが、他のケーブルテレビジョンのオペレータから受信することを許可された複数の

の加入者端末における複数の暗号キーとは異なることを特徴とする請求項17記載のシステム。

【請求項20】 ケーブルテレビジョンシステムであって、

ケーブルテレビジョンシステムは、(a) ケーブルテレビジョン分配ネットワークと、(b) 個々の放送事業者装置からのみ受信することが許可された複数の加入者端末のために定められた上記ネットワークを介してプログラムを送信するように設けられた複数のケーブルテレビジョンの放送事業者装置と、(c) 上記ネットワークと接続された複数の加入者端末とを備え、上記各加入者端末は、暗号キーを含み、上記各コードはある特定の放送事業者に対して唯一であり、(d) 上記各端末に設けられ、1つのプログラムを選択し、上記暗号キーから得られた暗号化されたイベント要求コードを得るための手段と、(e) 上記複数の放送事業者装置に設けられ、1つのイベントに対して唯一であって個々の特定の放送事業者に対して唯一であるパスワードを発生するための手段と、(f) 1つのプログラムが選択された1つの端末に上記パスワードを印加し、上記プログラムが選択された端末で、選択されたプログラムの表示を制御し、これによって、他の放送事業者によって放送された複数のプログラムを他の端末で表示されることを禁止するための手段とを備えたことを特徴とするケーブルテレビジョンシステム。

【請求項21】 ネットワークと、

上記ネットワークと接続され、異なったオペレータのうちの特定のオペレータによって提供された複数の信号を受信することが許可された複数の加入者端末と、  
上記複数の信号の上記複数の加入者による受信を、上記複数の加入者端末が許可された上記複数のオペレータのうちの特定のオペレータによって提供された上記複数の信号の上記複数の加入者による受信に限定するための手段とを備えたことを特徴とするケーブルテレビジョンシステム。

【請求項22】 上記限定するための手段は、上記複数のプログラムをデスクランブルするためのパスワードによってイネーブルされたデスクランブルコードであり、上記パスワードは、もう1つの別の特定の端末に対して無効である1つの特定の端末のための1つの特定のオペレータによって提供されることを特徴とする請求項21記載のシステム。

【請求項23】 上記もう1つの別の特定の端末は、上記もう1つの特定のオペレータによって複数の信号を受信することが許可された端末であることを特徴とする請求項22記載のシステム。

【請求項24】 複数の信号を種々の複数の加入者に分配するための方法であって、上記方法は、(a) 複数の加入者を、プログラム分配ネットワークから複数のプログラムを受信するための1つのプログラム分配ネットワ

ークに接続することと、(b)複数のプログラム供給装置を上記ネットワークに接続することと、(c)ある特定のプログラム供給装置に係るコードを種々の複数の加入者端末のそれぞれにダウンロードし、上記コードに係る複数の加入者端末に格納することと、(d)特定の分離チャンネルで上記複数のプログラム供給装置からの複数のプログラムを上記ネットワークに送信することと、(e)上記複数のコードを用いて、特定の複数の加入者端末によって関係するプログラム供給装置からのみの特定のプログラムの受信を可能にすることを含むことを特徴とする方法。

【請求項25】 上記複数の信号を人工衛星送信機を介して分配することを含むことを特徴とする請求項24記載の方法。

【請求項26】 上記複数の信号をローカルの送信機を介して分配することを含むことを特徴とする請求項24記載の方法。

【請求項27】 上記複数の信号をワイドエリアの光ファイバネットワークを介して分配することを含むことを特徴とする請求項24記載の方法。

【請求項28】 複数の信号を、ネットワークに接続された有効な複数の加入者に分配するための方法であって、プログラム販売促進コードに基づいてプログラム供給装置からプログラムを要求することと、上記ネットワークに接続された1つの端末と、上記プログラムとに対して唯一であるパスワードを供給することと、上記パスワードを上記端末に対して印加して、上記選択されたプログラムを実行することを含むことを特徴とする方法。

【請求項29】 複数の信号を、ネットワークに接続された有効な複数の加入者に分配するための方法であって、プログラム販売促進コードに基づいてペーパービューサーバー上のプログラムを供給するプログラム供給装置からのプログラムを要求することと、上記ネットワークに接続された1つの端末と、上記ペーパービューサーバーとに対して唯一であるパスワードを供給することと、上記パスワードを上記端末に対して印加して、上記選択されたプログラムを実行することを含むことを特徴とする方法。

【請求項30】 上記パスワードはまた上記プログラムに対して唯一であることを特徴とする請求項29記載の方法。

【請求項31】 複数の信号を有効な複数の加入者に分配するための方法であって、

(a) 中央局において、有効な複数の加入者端末識別コードを格納することと、

(b) それぞれが特定の販売促進コードに関連する複数の加入者に利用可能な複数のサービスの販売促進を放送することと、(c) 上記複数のサービスのうちの1つを選択し、選択されたサービス販売促進コードを加入者のロケーションにおける端末に入力することと、(d) 上記選択された販売促進コードの入力に回答して、上記端末と関連する識別番号を自動的に読み出すことと、

(e) 上記識別番号と上記選択された販売促進コードとを処理し、そこからイベント要求コードを発生することと、(f) 上記イベント要求コードを認証センタに提供することと、(g) 上記認証センタにおいて、上記イベント要求コードを処理し、上記加入者端末識別コードをアクセスし、上記端末と上記選択された販売促進コードとに唯一であるパスワードを提供することと、(h) 上記パスワードを上記加入者のロケーションにおける端末に入力することと、(i) 上記パスワードの入力に回答して、上記選択された販売促進コードに対応する上記分配された複数の信号の1つを利用するサービスに対するアクセスを、上記加入者に提供することを含むことを特徴とする方法。

【請求項32】 複数の信号を有効な複数の加入者に分配するための方法であって、(a) 加入者端末において、サービスに係るプログラムコードと、上記端末の識別に係るアドレスコードとをアクセスすることによって上記複数の信号を利用するサービスのための要求コードを発生し、上記複数のコードを処理してサービス要求コードを発生することと、(b) 上記サービス要求コードを提供することによって、中央端末からの上記サービスを要求することと、(c) 上記中央端末において、上記サービス要求コードを処理し、上記アドレスコードと上記プログラムコードとの有効性をチェックし、パスワードを発生することと、(d) 上記パスワードを上記加入者端末に入力し、上記複数の信号に対するアクセスを提供することに回答して、上記サービスを提供することを含むことを特徴とする方法。

【請求項33】 上記プログラムコードは、上記サービスの1つのサーバーに対して唯一であることを特徴とする請求項32記載の方法。

【請求項34】 上記サービスは、ペーパービューのプログラム信号の提供であることを特徴とする請求項33記載の方法。

【請求項35】 ケーブルテレビジョンシステムであって、上記ケーブルテレビジョンシステムは、

(a) 複数の加入者端末を備え、上記各加入者端末は、(i) 端末識別コードを格納するための手段と、(ii) プログラム識別コードを格納するための手段と、(iii) 上記複数のコードを処理し、それによってプログラム要求コードを発生するための手段と、(iv) 複数のプログラムを表示し、上記プログラム要求コードを表示す

るためのディスプレイと、(v) パスワードを受信し、これにตอบสนองして、プログラムをディスプレイ上に表示するために上記ディスプレイに入力するための手段と、

(b) ヘッドエンドと、上記ヘッドエンドに接続されたCATVネットワークとを備え、上記ヘッドエンドは上記プログラムを上記CATVネットワークを介して上記複数の加入者端末に送信し、

(c) 中央局を備え、上記中央局は、(i) 上記プログラム要求コードを受信し、そこから上記プログラム識別コードと上記端末識別コードとを決定するための手段と、(ii) 上記決定されたプログラムと端末識別コードとの有効性を認証するための手段と、(iii) 上記決定されたプログラムと端末識別コードとの有効性の認証にตอบสนองして、上記パスワードを発生するための手段とを備えたことを特徴とするケーブルテレビジョンシステム。

【請求項36】 ケーブルテレビジョンシステムであつて、

上記ケーブルテレビジョンシステムは、(a) ケーブルテレビジョン分配ネットワークと、(b) 個々の放送事業者装置からのみ受信することが許可された複数の加入者端末のために定められた上記ネットワークを介して複数のプログラムを送信するように設けられた複数のケーブルテレビジョンの放送事業者装置と、(c) 上記ネットワークと接続された複数の加入者端末とを備え、上記各加入者端末は、第1のコードを含み、上記各コードはある特定の放送事業者に対して唯一であり、(d) 上記各端末で設けられ、1つのプログラムを選択し、上記第1のキーから得られたイベント要求コードを得るための手段と、(e) 上記複数の放送事業者装置に設けられ、1つのイベントに対して唯一であつて個々の特定の放送事業者に対して唯一であるパスワードを発生するための手段と、(f) 1つのプログラムが選択された1つの端末に上記パスワードを印加し、上記プログラムが選択された端末で、選択されたプログラムの表示を制御し、これによって、他の放送事業者によって放送された複数のプログラムを他の端末で表示されることを禁止するための手段とを備えたことを特徴とするケーブルテレビジョンシステム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、ケーブル（有線）テレビジョンシステム（以下、CATVシステムという。）の有効な加入者に信号を分配するための方法及びCATVシステムに関し、特に、テレビジョンペイパービューシステムにおいて有用に用いられる当該方法とCATVシステムに関する。

【0002】

【従来の技術及び発明が解決しようとする課題】 有料テレビジョンシステムは、一般に、次の2つのアテゴリーのうちの1つに分類することができる。

(a) 加入者がある時間の間にあるチャンネルにおいて伝送されるすべての信号を視聴するための月極め料金を支払う場合、もしくは、(b) 選択されたプログラムが各要求したプログラムのための料金を支払うある加入者によって視聴され、すなわち、加入者がペイパービュー（pay per view）を行う場合。すなわち、ペイパービュー方式は視聴した番組（プログラム）の数に応じて加入者が料金を支払う。上記第1のカテゴリにおいては、視聴が許可された加入者の伝送線路からフィルタ装置が除去されるか、もしくは、デスクランブル信号がヘッドエンドから加入者端末におけるデコーダにダウンロードされる。上記第2のカテゴリにおいては、特定のプログラムにに対して限定されたデコード信号が電話回線を介して又はケーブルネットワークを介してアドレス指定されたデコーダに対して伝送される。

【0003】 各時間において加入者がサービスの加入者契約をしたとき又は当該サービスをキャンセルしたとき、もしくは当該サービスに対する支払いを怠ったときに、多数の住民数のエリアにおける各加入者のロケーションで各箇所フィルタ装置を除去し又は付加するために、サービスマンを派遣することは非常に高価である。さらに、特定のプログラムのために、又は特定の時間の間においてデスクランブルするためのコード（以下、デスクランブルコードという。）を提供するために、個々のアドレスによって各加入者端末をアドレス指定するための必要条件是、所望のシステムよりはより小さいシステムであるということが分かってきた。なぜならば、不足している帯域幅を利用しており、長い時間にわたってコードのダウンロードを必要とするために低速であるためである。

【0004】 さらに、そのようなシステムは、複数のケーブルテレビジョンの会社によって使用される共通のケーブルテレビジョンネットワークを用いて使用することができなかった。なぜならば、1つのケーブルテレビジョンの会社に対する1人の加入者がもう1つのケーブルテレビジョンの会社に電話をしてデスクランブルのコードのダウンロードを得ることにより、加入者に対して権利が与えられなかった信号を受信することができるが、1番目のケーブルテレビジョンの会社から当該加入者からの収益を剥奪するからである。

【0005】 さらに、比較的貧弱なセキュリティのために、そのようなシステムは、例えばバンキングサービス、パーソナルサービス、又は商品の注文サービスなど、本来のケーブルテレビジョンのサービス以外の他のサービスを提供するための使用に対して適してはいない。この場合において、課金ステートメントなど課金に関する情報が加入者のテレビジョンディスプレイ装置上に表示されることが所望される。

【0006】 本発明の目的は以上の課題を解決し、端末の基礎によって1つのヘッドエンドから1つの端末に対

して、デスクランブルコード、又は加入者端末をイネーブルするためのコード（以下、イネーブルコードという。）をダウンロードすることを必要とせず、サービス提供者が、例えば、バンキング、商品の注文、パーソナルな情報の記憶検索などのサービスを提供することを可能にして用いることができる、ペーパービュー又はそれに等価なサービスを提供するためのCATVシステムの有効な加入者に信号を分配するための方法及びCATVシステムを提供することにある。

【0007】

【課題を解決するための手段】本発明に係る請求項1記載の複数の信号を有効な複数の加入者に対して分配するための方法は、（a）中央局において、有効な複数の加入者端末識別コードを記憶することと、（b）それぞれが特定の販売促進コードと関連する複数の加入者に利用可能な複数のサービスの販売促進を放送することと、

（c）上記複数のサービスの1つを選択しかつ選択されたサービスの販売促進コードを加入者のロケーションにおける1つの端末に入力させることと、（d）上記選択された販売促進コードの入力に回答して、上記端末と関連する識別番号を自動的に読み出すことと、（e）暗号化アルゴリズムに従って上記識別番号と上記選択された販売促進コードとを処理し、かつそこから暗号化されたイベント要求コードを発生することと、（f）上記イベント要求コードを認証センタに供給することと、（g）上記認証センタにおいて、上記イベント要求コードを暗号解読し、かつ上記端末と上記選択された販売促進コードに唯一であるパスワードを供給することと、（h）上記パスワードを上記加入者のロケーションにおける端末に入力させることと、（i）上記パスワードの入力に回答して、上記選択された販売促進コードに対応する分配された複数の信号の1つを利用する1つのサービスに対するアクセスを上記端末に提供することを含むことを特徴とする。

【0008】また、請求項2記載の方法は、請求項1記載の方法において、ケーブルネットワークによる上記複数のサービスを上記複数の加入者に分配することを含むことを特徴とする。

【0009】さらに、請求項3記載の方法は、請求項1記載の方法において、上記識別番号は固定され、上記各端末におけるROMとスイッチの一群のうちの1つに格納されたことを特徴とする。

【0010】さらに、請求項4記載の方法は、請求項2記載の方法において、上記識別番号は変化可能であり、RAMに格納され、上記各端末と関連する固定されたアドレスをさらに含み、上記識別番号は、上記固定されたアドレスによって識別された加入者にアドレス指定されたケーブルを介して受信されることを特徴とする。

【0011】またさらに、請求項5記載の方法は、請求項2記載の方法において、上記複数の端末のそれぞれに

暗号キーを送信することと、上記暗号キーを上記各端末で格納することを含むことを特徴とする。

【0012】また、請求項6記載の方法は、請求項2記載の方法において、上記各端末は固定されたアドレスを有し、上記方法は、複数の暗号キーを上記固定されたアドレスによって識別された上記複数の端末に送信することと、上記各端末で現在の暗号キーを格納することを含むことを特徴とする。

【0013】さらに、請求項7記載の方法は、請求項5記載の方法において、上記複数の販売促進コードに關係する複数のプログラムコードを上記複数の端末のそれぞれに送信することと、上記販売促進コードとしてのプログラムコードと、端末識別コードとを、格納された暗号キーを用いて暗号解読しかつ符号化して上記イベント要求コードを発生することを含むことを特徴とする。

【0014】またさらに、請求項8記載の方法は、請求項6記載の方法において、上記各固定された識別番号は、上記各端末におけるROMに格納されることを特徴とする。

【0015】また、請求項9記載の方法は、請求項7記載の方法において、上記複数のサービスのうちの少なくとも1つはペーパービューテレビジョン信号であることを特徴とする。

【0016】さらに、請求項10記載の方法は、請求項9記載の方法において、上記テレビジョン信号はスクランブルされ、上記アクセスを提供するステップは、上記パスワードの入力時に、上記信号をデスクランブルすることを含むことを特徴とする。

【0017】本発明に係る請求項11記載の複数の信号を有効な複数の加入者に対して分配するための方法は、

（a）加入者端末において、サービスに關係する格納されたプログラムコードと、上記端末の識別に關係するアドレスコードとをアクセスすることによって、上記複数の信号を利用するサービスのための要求コードを発生し、かつ端末暗号キーを用いて上記複数のコードを暗号化してサービス要求コードを発生することと、（b）上記サービス要求コードを提供することによって中央端末からの上記サービスを要求することと、（c）上記中央端末において、上記サービス要求コードを暗号解読し、上記アドレスコードと上記プログラムコードとの有効性をチェックし、かつ1つのパスワードを発生することと、（d）上記パスワードを上記加入者端末に入力し、上記複数の信号に対するアクセスを提供することに回答して、上記サービスを提供することを含むことを特徴とする。

【0018】また、請求項12記載の方法は、請求項11記載の方法において、ヘッドエンドから上記加入者端末に暗号キーをダウンロードすることを含むことを特徴とする。

【0019】さらに、請求項13記載の方法は、請求項

12記載の方法において、ケーブル分配器又は複数のオペレータ暗号キーは、各加入者端末が端末アドレスによって識別された複数の加入者端末にダウンロードされることを特徴とする。

【0020】またさらに、請求項14記載の方法は、請求項13記載の方法において、複数の放送事業者によって上記複数の信号を供給することと、同一の暗号キーを各放送事業者に登録されたすべての加入者にダウンロードすることを含み、異なった暗号キーが異なった放送事業者に登録された複数の加入者に供給されることを特徴とする。

【0021】また、請求項15記載の方法は、請求項14記載の方法において、上記複数の信号は、すべての上記複数の放送事業者によって共通に使用されたケーブルネットワークを介して分配されることを特徴とする。

【0022】さらに、請求項16記載の方法は、請求項11記載の方法において、上記要求コードは、加入者に注意するためにテレビジョンのスクリーン上に表示され、上記サービスが要求されることを特徴とする。

【0023】本発明に係る請求項17記載のケーブルテレビジョンシステムは、

(a) 複数の加入者端末を備え、上記各加入者端末は、  
(i) 端末識別コードを格納するための手段と、(ii) プログラム識別コードを格納するための手段と、(iii) 暗号キーを格納するための手段と、(iv) 暗号化アルゴリズムに従って上記複数のコードと上記キーとを処理することにより、プログラム要求コードを発生するための手段と、(v) 複数のプログラムを表示し、かつ上記プログラム要求コードを表示するためのディスプレイと、(vi) 1つのパスワードを受信し、それに応答して通過すべきプログラムを上記ディスプレイ上に表示するために上記ディスプレイに入力するための手段とを備え、

(b) ヘッドエンドと、上記ヘッドエンドに接続されたCATVネットワークとを備え、上記ヘッドエンドは、上記プログラムのスクランブルされた信号を上記CATVネットワークを介して上記複数の加入者端末に送信し、

(c) 中央局を備え、上記中央局は、(i) 上記プログラム要求コードを受信するための手段と、(ii) 上記プログラム要求コードを暗号解読し、そこから上記プログラム識別コードと上記端末識別コードを決定するための手段と、(iii) 上記決定されたプログラムと端末識別コードとの有効性を認証するための手段と、(iv) 上記決定されたプログラムと端末識別コードの有効性の認証に応答して上記パスワードを発生するための手段とを備えたことを特徴とする。

【0024】また、請求項18記載のシステムは、請求項17記載のシステムにおいて、上記中央局における上記受信するための手段は、電話回線に接続され、加入者

によって上記電話回線を介して入力された上記プログラム要求コードの各ディジットを検出するための自動タッチトーン信号検出回路と、上記パスワードの音声化された音声信号を合成的に発生し、かつ当該音声信号を上記加入者によって受信するために上記電話回線に印加するための音声応答装置とを備えたことを特徴とする。

【0025】さらに、請求項19記載のシステムは、請求項17記載のシステムにおいて、上記システムは、複数の中央局を備え、上記各中央局は異なったケーブルテレビジョンのオペレータによって操作され、上記ケーブルテレビジョンのオペレータのすべては、同一のネットワーク上の複数のプログラムを複数の加入者端末の一群に分配し、上記複数の加入者端末における複数の暗号キーは、すべて同一である1人のケーブルテレビジョンのオペレータから受信することを許可されるが、他のケーブルテレビジョンのオペレータから受信することを許可された複数の加入者端末における複数の暗号キーとは異なることを特徴とする。

【0026】本発明に係る請求項20記載のケーブルテレビジョンシステムは、(a) ケーブルテレビジョン分配ネットワークと、(b) 個々の放送事業者装置からのみ受信することが許可された複数の加入者端末のために定められた上記ネットワークを介してプログラムを送信するように設けられた複数のケーブルテレビジョンの放送事業者装置と、(c) 上記ネットワークと接続された複数の加入者端末とを備え、上記各加入者端末は、暗号キーを含み、上記各コードはある特定の放送事業者に対して唯一であり、(d) 上記各端末に設けられ、1つのプログラムを選択し、上記暗号キーから得られた暗号化されたイベント要求コードを得るための手段と、(e) 上記複数の放送事業者装置に設けられ、1つのイベントに対して唯一であって個々の特定の放送事業者に対して唯一であるパスワードを発生するための手段と、(f) 1つのプログラムが選択された1つの端末に上記パスワードを印加し、上記プログラムが選択された端末で、選択されたプログラムの表示を制御し、これによって、他の放送事業者によって放送された複数のプログラムを他の端末で表示されることを禁止するための手段とを備えたことを特徴とする。

【0027】本発明に係る請求項21記載のケーブルテレビジョンシステムは、ネットワークと、上記ネットワークと接続され、異なったオペレータのうちの特定のオペレータによって提供された複数の信号を受信することが許可された複数の加入者端末と、上記複数の信号の上記複数の加入者による受信を、上記複数の加入者端末が許可された上記複数のオペレータのうちの特定のオペレータによって提供された上記複数の信号の上記複数の加入者による受信に限定するための手段とを備えたことを特徴とする。

【0028】また、請求項22記載のシステムは、請求

項21記載のシステムにおいて、上記限定するための手段は、上記複数のプログラムをデスクランブルするためのパスワードによってイネーブルされたデスクランブルコードであり、上記パスワードは、もう1つの別の特定の端末に対して無効である1つの特定の端末のための1つの特定のオペレータによって提供されることを特徴とする。

【0029】さらに、請求項23記載のシステムは、請求項22記載のシステムにおいて、上記もう1つの別の特定の端末は、上記もう1つの特定のオペレータによって複数の信号を受信することが許可された端末であることを特徴とする。

【0030】本発明に係る請求項24記載の複数の信号を種々の複数の加入者に分配するための方法は、(a) 複数の加入者を、プログラム分配ネットワークから複数のプログラムを受信するための1つのプログラム分配ネットワークに接続すること、(b) 複数のプログラム供給装置を上記ネットワークに接続すること、(c) ある特定のプログラム供給装置に関係するコードを種々の複数の加入者端末のそれぞれにダウンロードし、上記コードを関係する複数の加入者端末に格納すること、(d) 特定の分離チャンネルで上記複数のプログラム供給装置からの複数のプログラムを上記ネットワークに送信すること、(e) 上記複数のコードを用いて、特定の複数の加入者端末によって関係するプログラム供給装置からのみの特定のプログラムの受信を可能にすることを含むことを特徴とする。

【0031】また、請求項25記載の方法は、請求項24記載の方法において、上記複数の信号を人工衛星送信機を介して分配することを含むことを特徴とする。

【0032】さらに、請求項26記載の方法は、請求項24記載の方法において、上記複数の信号をローカルの送信機を介して分配することを含むことを特徴とする。

【0033】またさらに、請求項27記載の方法は、請求項24記載の方法において、上記複数の信号をワイドエリアの光ファイバネットワークを介して分配することを含むことを特徴とする。

【0034】本発明に係る請求項28記載の複数の信号を、ネットワークに接続された有効な複数の加入者に分配するための方法は、プログラム販売促進コードに基づいてプログラム供給装置からプログラムを要求すること、上記ネットワークに接続された1つの端末と、上記プログラムとに対して唯一であるパスワードを供給すること、上記パスワードを上記端末に対して印加して、上記選択されたプログラムを実行することを含むことを特徴とする。

【0035】本発明に係る請求項29記載の複数の信号を、ネットワークに接続された有効な複数の加入者に分配するための方法は、プログラム販売促進コードに基づいてペーパービューサーバー上のプログラムを供給する

プログラム供給装置からのプログラムを要求すること、上記ネットワークに接続された1つの端末と、上記ペーパービューサーバーとに対して唯一であるパスワードを供給すること、上記パスワードを上記端末に対して印加して、上記選択されたプログラムを実行することを含むことを特徴とする。

【0036】また、請求項30記載の方法は、請求項29記載の方法において、上記パスワードはまた上記プログラムに対して唯一であることを特徴とする。

【0037】本発明に係る請求項31記載の複数の信号を有効な複数の加入者に分配するための方法は、(a) 中央局において、有効な複数の加入者端末識別コードを格納すること、(b) それぞれが特定の販売促進コードに関連する複数の加入者に利用可能な複数のサービスの販売促進を放送すること、(c) 上記複数のサービスのうちの1つを選択し、選択されたサービス販売促進コードを加入者のロケーションにおける端末に入力すること、(d) 上記選択された販売促進コードの入力に応答して、上記端末と関連する識別番号を自動的に読み出すこと、(e) 上記識別番号と上記選択された販売促進コードとを処理し、そこからイベント要求コードを発生すること、(f) 上記イベント要求コードを認証センタに提供すること、(g) 上記認証センタにおいて、上記イベント要求コードを処理し、上記加入者端末識別コードをアクセスし、上記端末と上記選択された販売促進コードとに唯一であるパスワードを提供すること、(h) 上記パスワードを上記加入者のロケーションにおける端末に入力すること、(i) 上記パスワードの入力に応答して、上記選択された販売促進コードに対応する上記分配された複数の信号の1つを利用するサービスに対するアクセスを、上記加入者に提供することを含むことを特徴とする。

【0038】本発明に係る請求項32記載の複数の信号を有効な複数の加入者に分配するための方法は、(a) 加入者端末において、サービスに関係するプログラムコードと、上記端末の識別に関係するアドレスコードとをアクセスすることによって上記複数の信号を利用するサービスのための要求コードを発生し、上記複数のコードを処理してサービス要求コードを発生すること、(b) 上記サービス要求コードを提供することによって、中央端末からの上記サービスを要求すること、(c) 上記中央端末において、上記サービス要求コードを処理し、上記アドレスコードと上記プログラムコードとの有効性をチェックし、パスワードを発生すること、(d) 上記パスワードを上記加入者端末に入力し、上記複数の信号に対するアクセスを提供することに応答して、上記サービスを提供することを含むことを特徴とする。

【0039】また、請求項33記載の方法は、請求項32記載の方法において、上記プログラムコードは、上記



サービスの1つのサーバーに対して唯一であることを特徴とする。

【0040】さらに、請求項34記載の方法は、請求項33記載の方法において、上記サービスは、ペーパービューのプログラム信号の提供であることを特徴とする。

【0041】本発明に係る請求項35記載のケーブルテレビジョンシステムは、

(a) 複数の加入者端末を備え、上記各加入者端末は、

(i) 端末識別コードを格納するための手段と、(ii) プログラム識別コードを格納するための手段と、(iii) 上記複数のコードを処理し、それによってプログラム要求コードを発生するための手段と、(iv) 複数のプログラムを表示し、上記プログラム要求コードを表示するためのディスプレイと、(v) パスワードを受信し、これにตอบสนองして、プログラムをディスプレイ上に表示するために上記ディスプレイに入力するための手段と、

(b) ヘッドエンドと、上記ヘッドエンドに接続されたCATVネットワークとを備え、上記ヘッドエンドは上記プログラムを上記CATVネットワークを介して上記複数の加入者端末に送信し、

(c) 中央局を備え、上記中央局は、(i) 上記プログラム要求コードを受信し、そこから上記プログラム識別コードと上記端末識別コードとを決定するための手段と、(ii) 上記決定されたプログラムと端末識別コードとの有効性を認証するための手段と、(iii) 上記決定されたプログラムと端末識別コードとの有効性の認証にตอบสนองして、上記パスワードを発生するための手段とを備えたことを特徴とする。

【0042】本発明に係る請求項36記載のケーブルテレビジョンシステムは、(a) ケーブルテレビジョン分配ネットワークと、(b) 個々の放送事業者装置からのみ受信することが許可された複数の加入者端末のために定められた上記ネットワークを介して複数のプログラムを送信するように設けられた複数のケーブルテレビジョンの放送事業者装置と、(c) 上記ネットワークと接続された複数の加入者端末とを備え、上記各加入者端末は、第1のコードを含み、上記各コードはある特定の放送事業者に対して唯一であり、(d) 上記各端末で設けられ、1つのプログラムを選択し、上記第1のキーから得られたイベント要求コードを得るための手段と、

(e) 上記複数の放送事業者装置に設けられ、1つのイベントに対して唯一であって個々の特定の放送事業者に対して唯一であるパスワードを発生するための手段と、

(f) 1つのプログラムが選択された1つの端末に上記パスワードを印加し、上記プログラムが選択された端末で、選択されたプログラムの表示を制御し、これによって、他の放送事業者によって放送された複数のプログラムを他の端末で表示されることを禁止するための手段とを備えたことを特徴とする。

【0043】

【作用】本発明によれば、端末の基礎によって1つのヘッドエンドから1つの端末に対して、デスクランブルコード、又は加入者端末をイネーブルコードをダウンロードすることを必要とせず、サービス提供者が、例えば、バンキング、商品の注文、パーソナルな情報の記憶検索などのサービスを提供することを可能にして用いることができる、ペーパービュー又はそれに等価なサービスを提供するためのCATVシステムの有効な加入者に信号を分配するための方法及びCATVシステムを提供する。

【0044】さらに、当該システムは、1つのケーブルテレビジョンの1人の加入者が別のもう1つのケーブルテレビジョンからプログラム又はサービスを注文することができるという危険なしに、複数のケーブルテレビジョンのオペレータによって、1つのネットワークの使用を容易にすることができる。

【0045】さらに、当該システムは、ケーブルネットワークの分配システムに対して必ずしもリンクする必要はないが、地域的な“放送中の”の放送事業者、衛星放送事業者などによって分配された加入者に対して有用な信号の提供を制御するために用いることができる。

【0046】当該システムはまた、例えば、特定のイネーブルコード又はデスクランブルコードを特にアドレス指定された端末に対して送信するためのヘッドエンドのための必要性なしに、特に許可された複数の加入者がデータを選択し又はデータを受信することを可能にし、信号を受信するために装備されるファクシミリ装置を介して当該データを、レポート、メッセージ、新聞、銀行のステートメント(声明又は公告)、確認のスリップ(伝票)などに変換することを可能にするために、“特定の地域に対して放送を行う(narrowcast)”ために用いることが適当である。

【0047】各端末は、加入者が1つのパスワードを端末に対して入力することによって、プログラムやサービスなどを指示する、特に要求されたシーケンスの信号を受信するために個々にイネーブル(動作可能と)されることが可能である。当該パスワードは、典型的には、押しボタン式(タッチトーン(登録商標))電話機によって入力され、合成音声応答システムによって上記パスワードを提供するイベント要求コードを認証した中央局から得られる。当該イベント要求コードは、加入者がある特定のプログラム又はサービスに対する要求を当該端末に入力した後に、当該加入者のテレビジョンスクリーン上に供給される。

【0048】あるペーパービューシステムにおいては、バーカー(客引き)チャンネルは、利用可能なプログラム及びサービスを、それぞれ番号付きで表示する。ある特定のプログラム又はサービスが所望されるとき、対応する番号が加入者によって加入者端末に入力される。その合間において加入者端末は、種々のプログラムやサー

ビスの識別コードを1つのメモリに格納しており、入力エラーが生じなかったか否かを確認するために、加入者によって入力された番号を、上記格納された番号を参照してチェックする。

【0049】次いで、加入者端末は、ROMやDIPスイッチなどにおいて格納することができる唯一の論理的又は物理的な端末アドレス（I.D.：識別アドレス又は端末ID）を検索し、上記選択されたプログラム又はサービスに対応するプログラム又はサービス識別コードを検索し、そして、暗号キーを利用して、当該暗号キーを用いるアルゴリズムを用いてプログラム番号や端末IDを処理して、テレビジョンスクリーン上に表示される、暗号化されたイベント要求コードを生成する。本発明に係る好ましい態様においては、コードが、演算チェック番号を含む14ディジットの長さを有しているが、これに限らず、ケーブルテレビジョンの会社の必要性に応じて、他のコード長さを用いることができる。次いで、加入者は、ペーパービューのイベントのための注文を出すアクションを初期化する。もし所望されるならば、用いられるディジットの数を減少させることができる自動的な番号識別（ANI：Automatic Number Identification）を用いてもよい。

【0050】注文を出すために、テレビジョンスクリーン上で加入者に対して表示されたイベント要求コードは、加入者による中央局に対する電話によって提供される。上記中央局はコードを暗号解読し、有効な加入者端末番号のリストを参照して端末番号をチェックし、上記プログラムコードをチェックし、例えば、加入者に対して、合成的に発生された音声の応答によって、上述のパスワードを提供する。次いで、加入者は、当該パスワードを端末に入力し、ここで、当該パスワードは、端末に対して、要求されたイベント、プログラム、サービスなどに対して特定のデスクランブルコードを提供するのみならず、端末に対して、あるプログラムの時間であって上記デスクランブルコードが出力されている時間の間にデスクランブルするための端末を認証し、また、好ましくは、上記端末に対して、ある特定の時刻であってある特定の時間の間において、テレビジョンディスプレイに対する出力を、バーカーチャンネルであるかもしれない要求されたチャンネルに自動的に切り換えるためのコマンドを提供し、これによって、プログラムが自動的に加入者に対して提供される。

【0051】一旦パスワードが加入者に提供されると、ペーパービューのイベントに対する注文は受理されて課金処理され、すなわち、勘定書に記入されて請求書が発行される。加入者は、当該イベントの開始まで、注文完了のキャンセルを行うためのオプションを有する。キャンセルの処理は、イベントの要求の処理と同様である。上記選択されたプログラムは、あなたがバーカーメニューにおける“キャンセル”オプションを選択したとき

に、テレビジョンスクリーン上にリストとして表示される。あなたがプログラムをキャンセルするように選択することができ、それが一旦実行されたならば、14ディジットのキャンセルコードが表示され、上記プログラムは当該端末において直ぐにキャンセルされる。上記14ディジットのコードは、ヘッドエンドに与えられて、プログラムが開始する前に勘定書をキャンセルする必要がある。上記テレビジョンスクリーン上に暗号化されたキャンセルコードを得た後に、加入者は、当該キャンセルコードを、注文を出すために用いられる電話番号とは異なる電話番号を用いて中央局に送信する。異なったパスワードは、加入者に与えられて、当該キャンセルの処理を完了実行するために端末に入力される。

【0052】実質的にセキュリティを提供する合理的な時間内で近年の暗号化技術を用いて発生された暗号化されたコードを暗号解読することは事実上不可能である。さらに、種々の端末に格納された暗号キーは、例えば、2カ月毎に、当該端末の永久アドレスによって個々がアドレス指定された端末に対してヘッドエンドから放送する（又は広く送信する）ことによってときどき変化させることができる。この場合においては、各端末は、選択されたプログラム又はサービスの直前にアドレス指定されることが必要ではなく、ピーク時間などにおいて必要とされる送信装置や帯域幅を節約することが明らかである。

【0053】さらに、種々のプログラムに関連する複数のコードはケーブルテレビジョンサービスの供給者によって選択されることができるので、典型的には、ペーパービュープログラムの送信より数時間前、又はただ1日前、もしくは2日前までに、バーカーチャンネルに対して提供されず、暗号化されたコードとパスワードの両方は、暗号キーのみならず、プログラム番号に依存し、分配されたペーパービュー信号をデスクランブルして詐欺行為で使用することを可能にするために、所定の時間内で違法な盗視聴者によって適当なパスワードを発生することは、事実上不可能である。

【0054】暗号キーは、同一のケーブルテレビジョンネットワーク又は他のメディア上で複数の信号を分配する幾つかのケーブルテレビジョンのオペレータのそれぞれに対して異ならせることができることに注意する必要がある。従って、加入者が加入契約したケーブルテレビジョンのオペレータと関連する、格納された特定の暗号キーを有する加入者端末は、もう1つのケーブルテレビジョンのオペレータの中央局装置によって認識されないイベント要求コードを発生するであろうし、もう1つのケーブルテレビジョンのオペレータの1人の加入者による要求に回答して、パスワードや有効なパスワードは発生されないであろう。このことは、すべてのケーブルテレビジョンのオペレータが1つのネットワークに接続されているこれら複数のケーブルテレビジョンのオペレー

タを分離するために加入者の分離を提供する。従って、ある全体の領域が1つのネットワーク内で、もしくは1つのネットワークの1つのグループ内で、多かれ少なかれ、接続されることができるように1つの設備が提供される。また、1つのオペレータに対して複数の加入者の独占又は独占権は存在せず、複数の加入者は、所望するどちらかのケーブルテレビジョンのオペレータを選択することができる。オーバーラップしている住民に対してサービスする複数のケーブルテレビジョンのオペレータは、1つのケーブルテレビジョンネットワークを2倍にする必要がなく、従って、かなりの費用を節約することができる。

【0055】本発明に係る1つの態様によれば、複数の信号を有効な複数の加入者に対して分配する方法は、中央局において少なくとも1つの加入者端末の有効な識別コードを格納することと、それぞれが特定の販売促進コードと関連する複数の加入者に利用可能な複数のサービスの販売促進を放送することと、上記複数のサービスの1つを選択しかつ選択されたサービスの販売促進コードを加入者のロケーションにおける1つの端末に入力させることと、上記選択された販売促進コードの入力に応答して上記端末と関連する識別番号を自動的に読み出すことと、暗号化アルゴリズムに従って上記識別番号と上記選択された販売促進コードとを処理して、そこから暗号化されたイベント要求コードを発生することと、上記イベント要求コードを認証センタに供給することと、認証センタにおいて、上記イベント要求コードを暗号解読することと、上記番号を上記有効な複数の識別コードを参照して認証して、上記端末に対して唯一のパスワードと上記選択された販売促進コードとを供給することと、上記パスワードを上記加入者のロケーションにおける端末に入力させることと、上記パスワードの入力に応答して上記選択された販売促進コードに対応する分配された複数の信号の1つを利用する1つのサービスに対するアクセスを上記端末に提供することを含む。

【0056】本発明に係るもう1つの態様によれば、複数の信号を有効な複数の加入者に対して分配するための方法は、加入者端末において、サービスに格納されたプログラムコードと、上記端末の識別に関するアドレスコードとをアクセスすることによって、上記複数の信号を利用するサービスのための要求コードを発生し、暗号キーを用いて上記複数のコードを暗号化してサービス要求コードを発生することと、上記サービス要求コードを供給することによって中央端末からのサービスを要求することと、中央端末において、上記サービス要求コードを暗号解読し、上記アドレスコードと上記プログラムコードとの有効性をチェックし、1つのパスワードを発生することと、上記パスワードを上記加入者端末に入力することと、複数の信号に対するアクセスの提供に応答してサービスを提供することを含む。

【0057】本発明に係るもう1つの態様によれば、ケーブルテレビジョンシステムは、複数の加入者端末を備え、上記各加入者端末は、端末識別コードを格納するための装置と、プログラム識別コードを格納するための装置と、暗号キーを格納するための装置と、暗号化アルゴリズムに従って上記複数のコードと上記キーを処理し、これによって、プログラム要求コードを発生するための装置と、複数のプログラムを表示しプログラム要求コードを表示するためのディスプレイと、1つのパスワードを受信し、それに応答してプログラムを上記ディスプレイ上に表示するために上記ディスプレイに入力するための装置とを含み、ヘッドエンドと、上記ヘッドエンドに接続されたCATVネットワークとを備え、上記ヘッドエンドは、上記プログラムのスクランブルされた信号を上記CATVネットワークを介して上記複数の加入者端末に送信し、さらに、中央局を備え、上記中央局は、上記プログラム要求コードを受信するための装置と、上記プログラム要求コードを暗号解読しそこから上記プログラム識別コードと上記端末識別コードを決定するための装置と、上記決定されたプログラムと端末識別コードとの有効性を認証するための装置と、上記決定されたプログラムと端末識別コードの有効性との認証に応答して上記パスワードを発生するための装置とを備える。

【0058】本発明に係るもう1つの態様によれば、ケーブルテレビジョンシステムは、ケーブルテレビジョン分配ネットワークと、個々の放送事業者装置からのみ受信することが許可された複数の加入者端末のために定められたネットワークを介してプログラムを送信するように設けられた複数のケーブルテレビジョンの放送事業者装置と、上記ネットワークと接続された複数の加入者端末とを備え、上記各加入者端末は、暗号キーを含み、上記各コードはある特定の放送事業者に対して唯一であり、上記各端末で設けられ1つのプログラムを選択し、上記暗号キーから得られた暗号化されたイベント要求コードを得るための装置と、上記複数の放送事業者装置に設けられ1つのイベントに対して唯一であって個々の特定の放送事業者に対して唯一であるパスワードを発生するための装置と、1つのプログラムが選択された1つの端末に上記パスワードを印加し、上記プログラムが選択された端末で選択されたプログラムの表示を制御し、これによって、他の放送事業者によって放送された複数のプログラムを他の端末で表示されることを禁止するための装置とを備える。

【0059】本発明に係るもう1つの態様によれば、ケーブルテレビジョンシステムは、1つのネットワークと、上記ネットワークに接続され異なった複数のオペレータのうちの特定の幾つかのオペレータによって提供された複数の信号を受信することが許可されたネットワークに接続された複数の加入者端末と、上記複数の加入者による信号の受信を、上記複数の加入者端末が許可され

た複数のオペレータのうちの特定の幾つかのオペレータによって提供されたプログラムの信号に制限するための装置とを備える。

【0060】本発明に係るもう1つの態様によれば、複数の信号を種々の加入者に分配するための方法は、複数の加入者を、ネットワークからのプログラムを受信するための1つのプログラム分配ネットワークに接続することと、複数のプログラム供給装置を上記ネットワークに接続することと、種々の加入者端末のそれぞれに、ある特定のプログラム供給装置に関係するコードをダウンロードし、上記コードを関係する加入者端末で格納することと、上記複数のプログラム供給装置からの複数のプログラムを特定の分離されたチャンネルで上記ネットワークに送信することと、上記複数のコードを用いて特定の加入者端末によって、関係するプログラム供給装置からのみの特定のプログラムの受信を可能にすることを含む。

#### 【0061】

【実施例】以下、図面を参照して本発明に係る実施例について説明する。図1は、本発明に係る一実施例のCATVシステムのブロック図である。本発明に関係がないテレビジョン分配システムの構造的な部分については当業者に公知であるので図示していないことが認識されるであろう。

【0062】ヘッドエンド1は、複数のCATV信号などの複数のプログラム信号を発生して、それらをメディア3を介して送信する。本発明に係る成功した試作品や本発明に係る好ましい実施例によれば、メディア3はケーブルテレビジョン分配ネットワークである。しかしながら、ヘッドエンド1は、例えば光ファイバネットワーク（情報ハイウェイ）などの衛星分配システム、通常のローカル放送、ワイドエリアネットワーク（WAN）を介して送信することができることが理解されるであろう。ヘッドエンド1によって送信された信号は商業的に、種々の複数のサービスを種々の複数の加入者に対して提供する、無料で分配された複数の信号、スクランブルされたテレビジョン信号又は他の信号をサポートしている。以下の記述は主として、無料で分配された複数の信号に関してであるが、ただスクランブルされた信号に関してなされている。従って、デスクランブラ／コンバータ7をバイパスし、もしくは複数の信号を例えばファクシミリポート又はコンピュータなどの入力などに提供する加入者端末の構成要素は図示されていない。しかしながら、1つの端末のこれらの構造的な概念は当業者に公知であって、ミッシェル・デュフレーヌ（Michel Dufresne）ほかによって発明されかつ1986年11月18日に付与された米国特許第4,623,920号において開示されている。

【0063】ヘッドエンド1から送信された複数の信号は、加入者端末5によって受信され、デスクランブラ／

コンバータ7の入力に供給される。もしデスクランブルコードがデスクランブラ／コンバータ7によって受信されていなかったならば、当該複数の信号はデスクランブラ／コンバータ7を通過しかつそのデスクランブラ／コンバータ7の出力に接続されたビデオモニタ9上に理解可能に表示されることがブロックされる。

【0064】動作中において、ヘッドエンド1は、複数の加入者によって利用可能な複数のサービスの販売促進のためのディスプレイ又は表示を、バーカーチャンネル上でスクランブルをかけずに送信し、ここで、複数の加入者のそれぞれは、関連する販売促進（又は広告）コードに関連している。当該複数のサービスは、ペイパービューのシステムにおいて視聴することが所望されるようなスクランブルされたテレビジョンプログラムを含み、もしくは、そのようなテレビジョンプログラムからなる。そのリストは、ペイパービューサービス供給装置2から収集することができる。

【0065】ある適当な時刻に、選択すべき複数のプログラムはまた他のチャンネルにおいて送信され、例えば、予め決められた時刻でヘッドエンド1から送信された、スクランブル済みの2つの異なったペイパービュー補助チャンネルが存在してもよい。

【0066】バーカーチャンネルはスクランブルされておらず、デスクランブラ／コンバータ7をバイパスするか、もしくはデスクランブルされるべき必要条件なしにデスクランブラ／コンバータ7を介して通過するかのいずれかであって、その後、ビデオモニタ9上に表示される。当該加入者はバーカーチャンネルを視聴し、ある1つのプログラムコードによって識別されたプログラムサービスを選択する。

【0067】次いで、当該加入者は当該プログラムコードを、例えば暗号化プロセッサ11に通過させる遠隔制御の手段によって、加入者端末5に入力する。

【0068】端末アドレスモジュール13は加入者端末5に関連しており、加入者端末5を論理的に識別する複数のディップスイッチの1つのグループ、又は、読出専用メモリ（ROM）に記憶された論理アドレス、又は、ファームウェアにおけるアドレス、又は幾つかの他の方法で永久的に記憶されたアドレスである。

【0069】加入者端末5はまた暗号キーを記憶又は格納するメモリ15を含む。

【0070】加入者がプログラムコードを、例えばペイパービュープログラムのような特に所望されたサービスのために加入者端末5に入力するときに、暗号化アルゴリズムはモジュール13から端末を識別するシリアル番号とメモリ15から暗号キーとをアクセスし、次いで、プログラムコードを利用して、上記暗号化アルゴリズムに従って上述のデータを処理し、暗号化されたイベント要求コードを発生する。本発明の好ましい実施例においては、イベント要求コードは14ディジットの長さを有

し、これについては詳細後述される。

【0071】また、好ましくは、バーカーチャンネル上で販売促進される複数のサービスのプログラム番号の信号は、デスクランブラ／コンバータ7からこれらの信号を受信するように接続されたプログラムメモリ17において格納されることが必要である。プロセッサ11がイベント要求コードを発生する前に、好ましくは、プロセッサ11は、上記プログラムメモリ17をアクセスし、格納されたプログラム番号を、加入者によって入力されたプログラムコードと比較する必要がある。もしプロセッサ11が入力されたプログラムコードを検出することに失敗したならば、明らかに、加入者は入力において誤入力（エラー）をしており、プロセッサ11はある信号をパス19を介してデスクランブラ／コンバータ7に送信して、あるメッセージをビデオモニタ9上に表示し、当該加入者に対して誤ったプログラムコードが入力されたことを知らせることができる。

【0072】プログラムコードが正しいと認証されたと仮定すると、例えば表示されたイベント要求コードを予め決められた電話番号に電話をかけるように加入者に対して知らせるなど、デスクランブラ／コンバータ7に接続されたビデオ表示信号発生器20によって発生された適当なメッセージを用いてビデオモニタ9上に加入者に対して表示するために、プロセッサ11によって発生されたイベント要求コードは、信号パス19を介してデスクランブラ／コンバータ7に通過される。

【0073】次いで、加入者はその加入者の電話機21を用いて後述されるようなチェックシステム24を含む中央局にダイヤルし、押しボタン式（タッチトーン）電話機又はそれに等価な装置によって暗号化されたイベント要求コードをキー入力し、当該イベント要求コードを電話回線23を介して中央局のチェックシステム24にある電話機25、モデム又はそれらに等価な装置に送信する。

【0074】加入者がその加入者の電話機21を用いてダイヤルするよりはむしろ、加入者端末5はモデムを含み、1つのコマンドを加入者端末5に入力したときに、上記モデムは中央局における対応するモデムに自動的にダイヤルするようにしてもよい。従って、そのような実施例においては、電話機21及び25は、互いに自動的に通信を行う2つのモデムに置き換えられる必要がある。

【0075】好ましい実施例においては、14ディジットコードは一般的なフォーマット：AAAAAEEE CBBBVの形式を有している。

【0076】ここで、AAAAAAは加入者端末5の端末アドレスからとられた6桁の十進数表示の数のフィールドであり、そこからイベントが注文されかつそこにプログラム又はサービスが送信される加入者端末の唯一の識別コードである。

【0077】EEEは加入者によって注文されたサービス又はペーパービューのイベントの番号を含むフィールドである。異なったイベント番号は各イベントと、当該イベントが提供された各日時に割り当てられる。例えば、奇数の月においては、イベント番号は、映画に対して001から399までの範囲で指定され、特別なイベントの対して400から499までの範囲で指定される。偶数の月においては、イベント番号は、映画に対して501から899までの範囲で指定され、特別なイベントの対して900から999までの範囲で指定される。

【0078】Cフィールドは、当該イベントが放送されるイベントの論理的なチャンネル番号を含む。その可能な値は、0から9までの間にある。上記のフォーマットを用いた小さなシステムにおいては、例えば、0はバーカーチャンネルと呼ばれる広告宣伝チャンネルであり、1は第1のペーパービューチャンネルであり、2は第2のペーパービューチャンネルである。複数の論理チャンネルはデスクランブラ／コンバータ7によって特定の複数のチャンネルに変換される。例えば、もし論理チャンネル1が選択され、復号化されることがイネーブルされ、チャンネル56は、復号化されかつ代表的なバーカーチャンネルであるチャンネル14上で表示されることが可能である第1のペーパービューチャンネルとして指定することができる。

【0079】BBBは、加入者端末5によって発生された課金（勘定書）コードである。課金コードはまた、加入者がその加入者自身の加入者端末を使用したときに当該コードを発生することを、中央の端末に対して認証を受けるために用いられる。当該BBB課金コードは加入者端末5における読出専用メモリ（ROM）において格納された暗号キーを用いて生成される。

【0080】Vは、前の13個の番号から計算される確認コードであり、ユーザがイベントのためのデータを入力したときに全く誤入力（エラー）をしていないことを中央の端末に対して示すために用いられる。

【0081】いま図1を参照すれば、イベント要求コードが電話機25又はそれに等価なモデムによって受信されたときに、そのことがチェックシステム24のインターフェース27において検出される。このことは、加入者によって入力されたイベント要求コードが、暗号解読システム29と結合する確認コードVを再構成することによって確認された又は有効にされたということである。もし無効である判断がなされたならば、加入者に対して再び入力するように求めるために、フィードバックメッセージが加入者に送信され、ここで、上記メッセージは、もし電話機が用いられたならば合成された音声メッセージであり、もしくは、モデムが用いられたならば加入者のテレビジョンのスクリーン上に表示するためのメッセージである。

【0082】チェックシステム24の一実施例においては、テーブル33が当該チェックシステム24にすべての有効な加入者のシリアル番号のリストを格納しており、テーブル35はそこに有効なプログラムのリストを格納している。プロセッサ36はテーブル33からデータを読み出し、1つの有効な端末アドレスが入力されたか否かが決定する。また、1つの有効なプログラム番号が入力されたことを確認するためにテーブル35をチェックする。

【0083】図2において図示されたもう1つの実施例においては、チェックシステム24Aは、イベント要求コードの有効性を検出し、インターフェース27に印加されるパスワードを発生するPPVサーバー31を備える。インターフェース27は合成的に形成された音声の言語で、電話機25において音響的に再生されるパスワードの番号及び／又はキャラクタを発生し、これによって、それが、イベント要求コードがキー入力された加入者に供給される。

【0084】とって代わって、パスワードは、上述のモデムに印加され、ローカルのモデムとデータ受信機37によってローカルの、デスクランブラ／コンバータ7によって認識可能な信号に変換された後に、デスクランブラ／コンバータ7に印加するために加入者端末5に直接に通過入力される。

【0085】もう1つの実施例によれば、テーブル33は不要にされる。暗号化されたイベント要求コードはチェックサムを含む。まず最初に当該チェックサムがイベント要求コードに対して正しいと決定することによって、もし正しければ、イベント要求コードを暗号解読し、1つの有効な加入者が1つのイベントを要求したことが決定される。もし上記コードが暗号解読することができないならば、無効な加入者として示され、もしくは、もしチェックサムが正しくないならば、エラーが生じているか又は伝送線路上で干渉が生じている。いずれの場合においても、イベントは拒否される。

【0086】もしコードが暗号解読されたならば、テーブル35は1つの有効なプログラムが選択されたか否かを決定するためにアクセスされる。とって代わって、テーブル35が用いられず、プログラムの有効性が加入者端末5でイベント要求コードの生成とともにチェックされるという仮定がなされる。

【0087】それは電話機25からパスワードを聞いた加入者であるということを仮定すれば、次いで、その加入者は、例えばパスワードを彼の端末の遠隔制御装置にキー入力することによって、パスワードを加入者端末5に入力する。当該パスワードはデータ受信機37で受信され、デスクランブラ／コンバータ7によって認識可能な信号に変換され、当該パスワードはそこに印加される。当該パスワードが受信された後に、暗号化プロセッサ11は逆の処理を実行して当該パスワードを暗号解読

する。その結果は、確認のために加入者局に保持されている元の要求コードと比較される。一致しないときは、無効なメッセージがスクリーン上に現れる。

【0088】もしパスワードが受理されたならば、これによって適当な時刻及び適当な時間の間で所望されたプログラムを表示する。

【0089】複数の加入者の有効性を制御するために、中央局のチェックシステム24は、図1において詳細に図示された課金装置39を含むSMS（サービス管理システム）を備える。課金装置39は、ケーブルテレビジョンのオペレータによって操作されるパーソナルコンピュータであることが可能である。良好なクレジット履歴を有し、又はあるプログラムに対して予め料金を支払っている（すなわち、プリペイドしている）特定のケーブルテレビジョンのオペレータに対して登録された複数の加入者は、テーブル33においてそのような有効な複数の加入者の複数の端末のアドレスを格納する課金装置39に入力される。

【0090】課金装置39はある特定のケーブルテレビジョンのオペレータと関係していることが可能であることに注意する必要がある。暗号キーは1つのデータチャンネルで各加入者に対して放送され、次いで、加入者端末5のメモリ15に記憶される。暗号キーは、好ましくは、ヘッドエンド1から、例えば2カ月や1カ月などの予め決められた時間間隔で変更される。暗号キーは課金装置39によって、又はネットワーク監視装置（図示せず。）によって発生されることが可能である。1つの暗号キーは、1つのケーブルテレビジョンのオペレータから複数のプログラムや複数のサービスを受信することが認証又は許可されたすべての加入者のために用いられることが可能である。

【0091】異なった複数の中央局24が、それぞれ各ケーブルのオペレータと関連するヘッドエンド1に接続することが可能である。しかしながら、すべての加入者端末5は同一のケーブルテレビジョンネットワークのメディア3に接続することが可能である。各ケーブルテレビジョンのオペレータと関連する複数の加入者端末を分離するために、ある特定のケーブルテレビジョンのオペレータから受信することを認証又は許可されたすべての加入者端末は同一の暗号キーを有する必要がある。異なった複数の暗号キーは、異なったケーブルテレビジョンのオペレータから受信することを認証又は許可された複数の加入者端末によって使用される。

【0092】上記の結果として、複数のイベント要求コードは、異なったケーブルテレビジョンのオペレータに認証又は許可された複数の加入者端末に関係する複数のケーブルテレビジョンのオペレータの中央局24によって認識されることはないであろう。従って、複数のケーブルテレビジョンのオペレータは同一のネットワークを使用することができ、無料のケーブルチャンネルとサー

ビスの送信をプールすることができる。また、異なった複数の暗号キーのために、それらのペーパービューの顧客は、全体として分離された状態で保持されることが可能である。このことは、それらの各システムのために異なったサービスの供給者と加入契約する種々のケーブルテレビジョンのオペレータに対して完全なセキュリティ（安全保障）を可能にする。

【0093】図4には、加入者端末5のより詳細なブロック図が図示されている。入力端子41はメディア3からの信号を受信し、それらの信号をコンバータ43に出力する。典型的には、コンバータ43は入力信号のチャンネルを、例えばビデオモニター9上の表示のためのチャンネル3に変換する。通常の複数の信号に対して、コンバータ43の出力は、スイッチ45を介してビデオモニター9のビデオ入力に印加するためにビデオ出力ライン46に通過出力される。

【0094】スイッチ45は、とって代わってコンバータ43の出力をデスクランブラ47に印加することができる。コンバータ43とスイッチ45とデスクランブラ47とは、バス51を介してマイクロプロセッサ49によって制御される。

【0095】遠隔制御される受信機53は、例えば、1人の加入者によって使用された遠隔制御の送信機からの複数の赤外線信号を受信し、当該複数の信号をデジタル形式の信号に変換し、それらの信号を、マイクロプロセッサ49によって受信するためにバス51に印加する。ランダムアクセスメモリRAM55は、加入者端末5の複数の機能を実行するときにマイクロプロセッサ49によって使用するための複数のプログラムを格納する。マイクロプロセッサ49はまた、ビデオモニター9上で表示するためにRAM55において格納されたデータをアクセスすることができ、次いで、ビデオ表示信号発生器56を用いて表示信号を生成した後、当該信号をデジタル／アナログコンバータ（以下、A/Dコンバータという。）57に印加し、当該A/Dコンバータ57においては、上記信号はビデオモニター9に表示することができ、当該信号は変調器48で変調されて出力ライン46に印加される。

【0096】上記の通常の動作は、ミッシェル・デュフレヌ（Michel Dufresne）ほかによって発明されかつ1986年11月18日に付与された米国特許第4,623,920号において開示され、これは参照することによってここに含まれる。

【0097】端末アドレスモジュール13はバス51に接続され、これによって、マイクロプロセッサ49は当該加入者端末5のシリアル番号をアクセスして読み出すことができる。さらに、暗号キーメモリ15はヘッドエンド1から送られた上述の暗号キーを格納することができる。

【0098】さらに、RAMプログラムメモリ17はマ

イクロプロセッサ49によってアクセスするためにバス51に接続される。

【0099】例えばチャンネル14であるバーカーチャンネル上の複数のプログラムはデスクランブラ47をバイパスすることによって表示される。バーカーチャンネルの垂直インターバル又はライン21において存在することが可能であるデータチャンネル上で送信されたデータがコンバータ43を介して印加され、もしくは、復調器（図示せず。）で復調されてバス51に出力される。このデータは、例えば、バーカーチャンネル上でリストアップされた複数のプログラムと関連するプログラム識別番号（又はプログラム識別子番号）である。マイクロプロセッサ49はこのデータをプログラムメモリ17に格納することを制御する。

【0100】プログラムリストはバーカーチャンネル上の加入者によって見られるときに、その加入者は、例えば彼の遠隔制御装置を用いて表示されかつ関連するプログラムコードを入力することによって、1つのプログラムを選択する。当該プログラムコードは、好ましくは、番号の前に例えば\*のような特定の識別子又は指定子キャラクタによって前に付与され、遠隔制御送信機によって遠隔制御受信機53に入力され、当該受信機53において、上記プログラムコードはデータに変換され、一時的にRAM55に格納される。マイクロプロセッサ49はプログラムコードを検出し、RAM55に格納された1つのプログラムを用いて、そこから、例えば、上記で参照されたEEEとなるディジットであるイベントコードを決定する。次いで、マイクロプロセッサ49はそれらのディジットをプログラムメモリ17に格納された対応するディジットを用いてチェックし、もし有効であるならば、RAM55に格納された暗号化アルゴリズムをアクセスする。

【0101】暗号化アルゴリズムを用いて処理するとき、マイクロプロセッサ49はモジュール13からシリアル番号をアクセスするとともに、RAM55に一時的に格納された上記選択されたプログラム番号をアクセスし、そして、好ましくは14ディジットのイベント要求コードを発生する。マイクロプロセッサ49は、上記イベント要求コードをビデオ表示信号発生器56を用いて表示可能な形式に定式化し、例えば確認の報告や命令などの説明のための幾つかのキャラクタを加算して、RAM55に格納されたデータをアクセスすることによって得られたある電話番号に対して電話をかけ、当該情報を上記ビデオモニター9上に表示するためにそれに印加する。上記加入者は、ビデオモニター9上で表示されたイベント要求コードを見ながら、指示された電話番号のディジットをダイヤルし、上述されたように、中央局24からパスワードを受信する。次いで、加入者は、遠隔制御受信機53によって受信されたパスワードを端末遠隔制御装置にキー入力する。当該パスワードは一時的にRA



M55に格納される。ここに格納されたプログラムを用いて、マイクロプロセッサ49は当該パスワードを、デスクランブラ47のために、イネーブル時刻、イネーブル時間、デスクランブルコード、及びチャンネル制御信号に復号化する。

【0102】さらに、以下のことが理解されるであろう。モデム61はバス51に接続することができ、イベント要求コードが加入者によって電話機にキー入力される代わりに、マイクロプロセッサ49の制御のもとで、モデム61は中央局24におけるモデムにダイヤルすることができ、イベント要求コードを当該モデムに自動的に送信することができ、次いで、そこからパスワードを受信し、当該パスワードをRAM55における格納及びマイクロプロセッサ49によってそのそれに続く使用のためにバス51に印加する。

【0103】クロック回路59によって指示された適当な時刻に、マイクロプロセッサ49は、スイッチ45をコンバータ43の出力をデスクランブラ47の入力に出力するように切り換え、上記格納されたデスクランブルコードをデスクランブラ47に印加し、コンバータ43に含まれるチューナを、パスワードにおいて指示された論理チャンネルによって指示されたある特定のスクランブルされたチャンネルから受信するように切り換え、コンバータ43に対して当該信号をバーカーチャンネルに又はいくつかの他の予め決められたチャンネルに出力させる。従って、要求されたチャンネルは変換され、スクランブルされ、そして、ビデオモニター9上での表示のために出力ライン46に印加される。

【0104】プログラムの指示された時間間隔の後に、マイクロプロセッサ49はスクランブルコード47を除去し、コンバータ43を前に同調又は切り換えられたチャンネルに戻すように切り換え、デスクランブラ47をバイパスするようにスイッチ45を切り換えることにより、ビデオモニター9に通常の無料のチャンネルを表示することを可能にする。

【0105】図4の実施例を参照して説明した複数のメモリは、もし所望されるならば効率的な方法で結合することができることが理解されるであろう。さらに、好ましくは、バックアップ電池は、電源故障の場合にメモリに格納されたデータを保持するために使用することが必要である。

【0106】図5は、複数のオペレータのネットワークを図示するブロック図である。複数のケーブルテレビジョンのオペレータ制御システム（以下、オペレータシステムという。）70A乃至70Nはそれぞれ、複数のプログラムを共通のネットワーク72を介してそれ自身の加入者の組に送信し、これらの加入者の組のそれぞれは同一の共通のネットワークに接続される。各加入者は、図4を参照して説明したような受信制御加入者端末を有する。各加入者は、有線リンク、マイクロ波リンク7

4、又は、複数の信号を受信するための他の手段によってメインヘッドエンド72から複数の信号を受信する。各ケーブルテレビジョンのオペレータシステムは、それ自身の加入者と、SMS（サービス管理システム）30A乃至30N及びサーバー31A乃至31Nとからなるプログラム許可及び認証システムを備える。各プログラム許可及び認証システムは、電話回線25のためのそれ自身の電話番号を有する。従って、各ケーブルテレビジョンのオペレータシステムは、それ自身のグループの加入者のための加入者端末と複数の暗号コードとを提供することができ、それ自身のパーカーチャンネル上でそれ自身の複数のプログラムコードを提供することができ、それ自身の複数の加入者に対してそれ自身のパスワードを提供することによって複数のプログラムを受信することを認証又は許可することができる。また、個々のケーブルテレビジョンのオペレータは、それに代わってSMS30やサーバー31を操作することについて、ヘッドエンド72のオペレータと請け負いの契約を行うことができることが認識されるであろう。個々のケーブルテレビジョンのオペレータが互いに干渉（インタフェア）している又はオーバーラップしているコードを使用しないことを確立するために、好ましくは、ヘッドエンド72のオペレータは、複数のオペレータシステムのそれぞれに対して個々に唯一のコードを割り当てる必要がある。複数のオペレータシステムは、上述したように共通のネットワーク72内で動作する。ある特定のケーブルテレビジョンのオペレータシステムに対して固有の唯一の共通コードを格納する種々の端末のそれぞれを用いるときに、ペーパービューのプログラム供給でない場合であっても、複数の加入者端末のそれぞれによるプログラムの受信は、関連するケーブルテレビジョンのオペレータシステムによって送り出されたプログラムに限定されることが可能である。なぜならば、コードは、種々のオペレータシステムのそれぞれによって唯一のスクランブルコードとともに送信された通常のプログラム信号のスクランブル処理を制御することができるからである。他のプログラムはヘッドエンド72から受理されることができ、上記ケーブルテレビジョンのオペレータシステムによってスクランブルされず、制限条件なしにすべての加入者によって一般に見るために、すべてのケーブルテレビジョンのオペレータシステムによって共通に送信される。上記ネットワークはCATVシステムである必要はないが、大勢の視聴者による受信のために任意の形式の信号を送信する大勢の視聴者のプログラム分配システムの任意の形式であってもよい。

【0107】この発明を理解する人は、変形の構造や実施例、もしくは上記の変形例を考えるかもしれない。この明細書に添付の請求の範囲に含まれるもののすべては、本発明の一部であると考える。

【0108】



【発明の効果】以上詳述したように本発明によれば、複数の信号を有効な加入者に対して分配する方法であって、(a) 中央局において加入者端末の有効な識別コードを記憶することと、(b) それぞれが特定の販売促進コードと関連する複数の加入者に利用可能な複数のサービスの販売促進を放送することと、(c) 上記複数のサービスの1つを選択しかつ選択されたサービスの販売促進コードを加入者のロケーションにおける1つの端末に入力させることと、(d) 上記選択された販売促進コードの入力に応答して上記端末と関連する識別番号を自動的に読み出すことと、(e) 暗号化アルゴリズムに従って上記識別番号と上記選択された販売促進コードとを処理し、かつそこから暗号化されたイベント要求コードを発生することと、(f) 上記イベント要求コードを認証センタに供給することと、(g) 上記認証センタにおいて、上記イベント要求コードを暗号解読し、かつ上記端末と上記選択された販売促進コードに唯一であるパスワードを供給することと、(h) 上記パスワードを上記加入者のロケーションにおける端末に入力させることと、(i) 上記パスワードの入力に回答して、上記選択された販売促進コードに対応する分配された複数の信号の1つを利用する1つのサービスに対するアクセスを上記端末に提供することを含む。

【0109】従って、端末の基礎によって1つのヘッドエンドから1つの端末に対して、デスクランブルコード、又は加入者端末をイネーブルコードをダウンロードすることを必要とせず、サービス提供者が、例えば、バンキング、商品の注文、パーソナルな情報の記憶検索などのサービスを提供することを可能にして用いることができる、ペイパービュー又はそれに等価なサービスを提供するためのCATVシステムの有効な加入者に信号を分配するための方法及びCATVシステムを提供することができる。

#### 【図面の簡単な説明】

【図1】 本発明に係る一実施例であるCATVシステムのブロック図である。

【図2】 図1におけるチェックシステムの変形例のブロック図である。

【図3】 図1におけるチェックシステムの別の変形例のブロック図である。

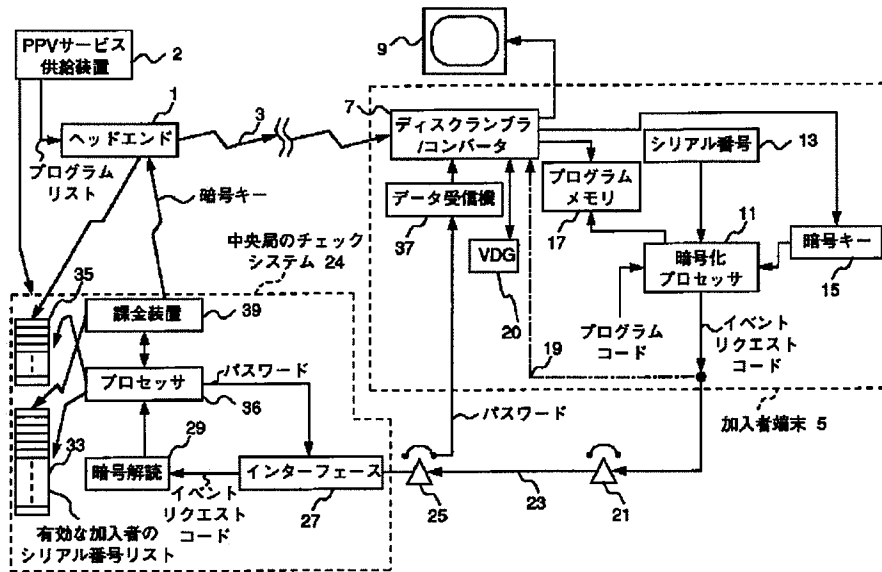
【図4】 図1における加入者端末の一部分のブロック図である。

【図5】 複数のオペレータのプログラム放送システムのブロック図である。

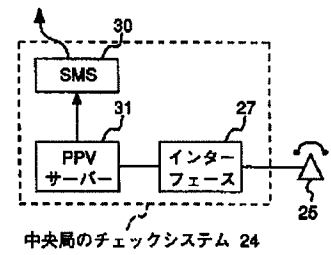
#### 【符号の説明】

1…ヘッドエンド、  
 2…PPV（ペイパービュー）サービス供給装置、  
 3…メディア、  
 5…加入者端末、  
 7…デスクランブラ／コンバータ、  
 9…ビデオモニタ、  
 11…暗号化プロセッサ、  
 13…端末アドレスモジュール、  
 15…暗号キーメモリ、  
 17…プログラムメモリ、  
 19…信号バス、  
 20…ビデオ表示信号発生器、  
 21…電話機、  
 23…電話回線、  
 24…中央局のチェックシステム、  
 25…電話機、  
 27…インタフェース、  
 29…暗号解読システム、  
 30, 30A乃至30N…SMS、  
 31, 31A乃至31N…PPVサーバー、  
 33…テーブル、  
 35…テーブル、  
 36…プロセッサ、  
 37…データ受信機、  
 39…課金装置、  
 41…入力端子、  
 43…コンバータ、  
 45…スイッチ、  
 46…ビデオ出力ライン、  
 47…デスクランブラ、  
 49…マイクロプロセッサ、  
 51…バス、  
 53…遠隔制御された受信機、  
 55…RAM  
 56…ビデオ表示信号発生器、  
 57…A／Dコンバータ、  
 59…クロック回路、  
 61…モデム、  
 70A乃至70N…ケーブルテレビジョンオペレータ制御システム、  
 72…共通ネットワーク、  
 74…マイクロ波リンク。

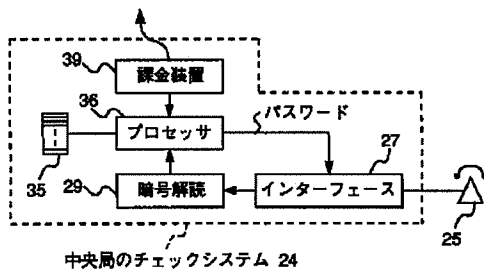
【図1】



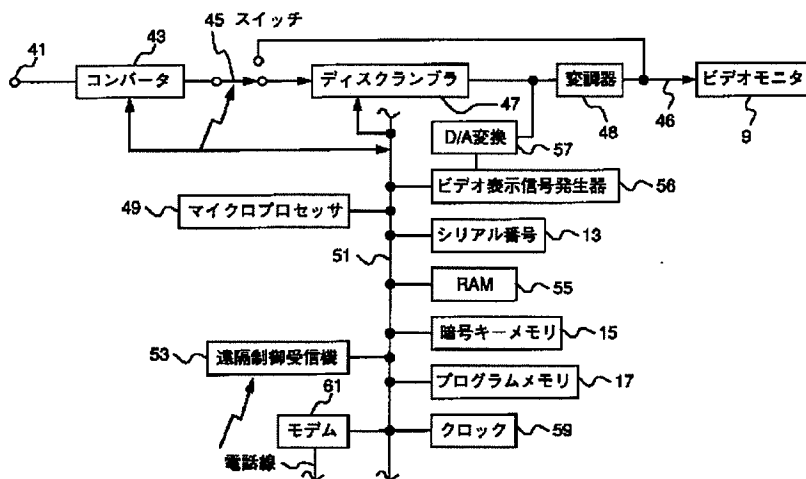
【図2】



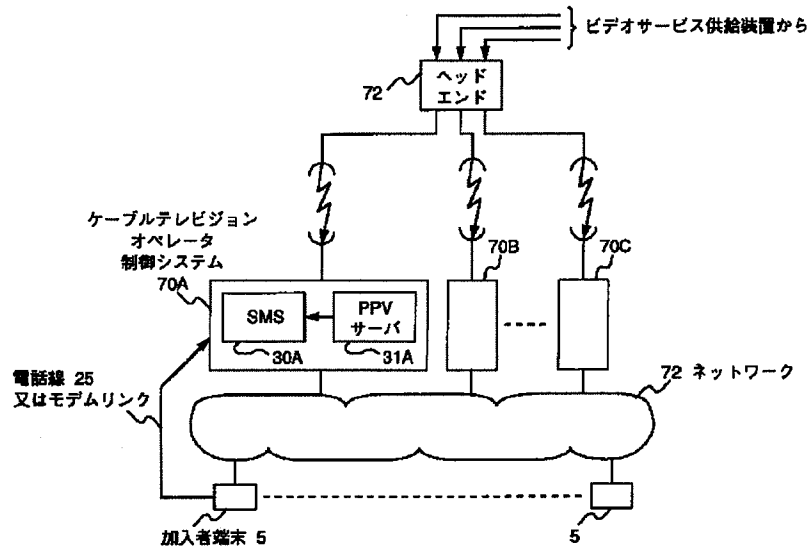
【図3】



【図4】



【図5】



フロントページの続き

(72)発明者 ジョセ・コリヴォー  
カナダ、アッシュ1ペ・2ヴェ3、ケベック、サン＝レオナル、アルフォンヌ＝デシャルダン8320番

(72)発明者 ミッシェル・デュフレーヌ  
カナダ、ジ4ベ・6カ4、ケベック、ブーシェヴィル、デュ・ペルシュ1096番

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-214283

(43)Date of publication of application : 20.08.1996

---

(51)Int.Cl.

H04N 7/173

---

(21)Application number : 07-017827 (71)Applicant : LE GROUPE VIDEOTRON LTD

(22)Date of filing : 06.02.1995 (72)Inventor : GARNEAU PIERRE  
CORRIVEAU JOSEE  
DUFRESNE MICHEL

---

(30)Priority

Priority number : 94 193410 Priority date : 07.02.1994 Priority country : US

---

(54) METHOD FOR DISTRIBUTING SIGNAL TO VALID SUBSCRIBER OF CATV SYSTEM AND CATV SYSTEM

(57)Abstract:

PURPOSE: To give access for services to terminals by making an authentication center decode enciphered event requesting codes and supply passwords to terminals.

CONSTITUTION: A central-station check system 24 selects one out of a plurality of services and makes a selected sales promoting code to be inputted to one subscriber's terminal 5. In response to the input of the selected sales promoting code the system 24 automatically reads out the identification number related to the terminal 5. Then the system 24 generates an enciphered event requesting code by processing the identification number and the selected sales promoting code in accordance with an enciphering algorithm. Thereafter the system 24 supplies the identification signal and sales promoting code to an authentication center and the center decodes 29 the enciphered event requesting code and sends a password to the terminal 5. In response to the input of the password to the terminal 5 one of a plurality of signals corresponding to the sales promoting code is sent to the accessing terminal 5.

---

CLAIMS

---

[Claim(s)]

[Claim 1] It is a method characterized by comprising the following for distributing two or more signals to two or more effective members and is (a) central office.

Two or more effective subscriber terminal identification codes are memorized.

(b) Each broadcasts sales promotion of two or more available services to two or more members connected with a specific sales promotion code.

(c) Make a sales promotion code of service which chose one of the above-mentioned services of two or more and was chosen input into one terminal in a member's location.

(d) Answer an input of a sales promotion code chosen [ above-mentioned ] and read automatically an identification number relevant to the above-mentioned terminal.

(e) Generate an event request code which processed a sales promotion code chosen [ above-mentioned ] with the above-mentioned identification number according to an encryption algorithm and was enciphered from there.

(f) Supply the above-mentioned event request code to an authentication center.

(g) A password which is only is supplied to a sales promotion code which deciphered the above-mentioned event request code and was chosen [ above-mentioned ] with the above-mentioned terminal in the above-mentioned authentication center.

(h) Provide the above-mentioned terminal with access to one service which answers making the above-mentioned password enter into a terminal in the above-mentioned member's location and an input of the (i) above-mentioned password and uses one of two or more of the distributed signals corresponding to a sales promotion code chosen [ above-mentioned ].

[Claim 2] A method according to claim 1 including distributing two or more above-mentioned services by a cable network to two or more above-mentioned members.

[Claim 3] a group of ROM [ in / the above-mentioned identification number is fixed and / each above-mentioned terminal ] and a switch -- a method according to claim 1 storing in one.

[Claim 4] A method according to claim 2 which the above-mentioned identification number can change is stored in RAM and is characterized by receiving the above-mentioned identification number via a cable addressed by member identified by an address fixed [ above-mentioned ] including further a fixed address relevant to each above-mentioned terminal.

[Claim 5] A method comprising according to claim 2:

A cryptographic key is transmitted to each of two or more above-mentioned terminals.

The above-mentioned cryptographic key is stored at each above-mentioned terminal.

[Claim 6] A method comprising according to claim 2:

Each above-mentioned terminal has the fixed address and a described method transmits two or more cryptographic keys to two or more above-mentioned

terminals identified by an address fixed [ above-mentioned ].

The present cryptographic key is stored at each above-mentioned terminal.

[Claim 7] Two or more program codes related to two or more above-mentioned sales promotion codes are transmitted to each of two or more above-mentioned terminals. A method according to claim 5 including deciphering a program code and a terminal identification code as the above-mentioned sales promotion code using a stored cryptographic key and coding and generating the above-mentioned event request code.

[Claim 8] A method according to claim 6 wherein a fixed each [ above-mentioned ] identification number is stored in ROM in each above-mentioned terminal.

[Claim 9] A method according to claim 7 wherein at least one of two or more above-mentioned services is a pay-per-view television signal.

[Claim 10] A method according to claim 9 including that a step which the scramble of the above-mentioned television signal is carried out and provides the above-mentioned access descrambles the above-mentioned signal at the time of an input of the above-mentioned password.

[Claim 11] It is a method characterized by comprising the following for distributing two or more signals to two or more effective members and is the (a) subscriber terminal.

A stored program code related to service.

A request code for service which uses two or more above-mentioned signals by accessing an address code related to discernment of the above-mentioned terminal is generated and two or more above-mentioned codes are enciphered using a terminal cryptographic key and a service request code is generated.

(b) Require the above-mentioned service from a central terminal by providing the above-mentioned service request code.

(c) In the above-mentioned central terminal decipher the above-mentioned service request code and check the validity of the above-mentioned address code and the above-mentioned program code and generate one password.

(d) Enter the above-mentioned password into the above-mentioned subscriber terminal and answer providing access to two or more above-mentioned signals and provide the above-mentioned service.

[Claim 12] A method of including downloading a cryptographic key in the above-mentioned subscriber terminal from a head end according to claim 11.

[Claim 13] A method according to claim 12 wherein each subscriber terminal downloads a cable distributor or two or more operator cryptographic keys to two or more subscriber terminals identified by a terminal address.

[Claim 14] It includes supplying two or more above-mentioned signals by two or more broadcasting organizations and downloading the same cryptographic key to all the members registered into each broadcasting organization. A method according to claim 13 supplying two or more members registered into a broadcasting organization from whom a different cryptographic key differed.

[Claim 15] A method according to claim 14 wherein two or more above-mentioned signals are distributed by two or more of all the above-mentioned broadcasting organizations via a cable network used in common.

[Claim 16] A method according to claim 11 wherein it is displayed on a screen of television in order to notice the above-mentioned request code about a member and the above-mentioned service is required.

[Claim 17] Cable television comprising:

A means to be cable television for the above-mentioned cable television to be provided with a subscriber terminal of (a) plurality and for each above-mentioned subscriber terminal store a (i) terminal identification code.

(ii) A means for storing a program identification code.

(iii) A means for storing a cryptographic key.

(iv) By processing a code and the above-mentioned key of the above-mentioned plurality according to an encryption algorithm a display for displaying a means for generating a program request code and a program of (v) plurality and displaying the above-mentioned program request code Receive one password in order to display a program which should answer it and should be passed on the above-mentioned display have a means for inputting into the above-mentioned display and (vi) The (b) head end Have a CATV network connected to the above-mentioned head end and the above-mentioned head end Transmit a signal with which the scramble of the above-mentioned program was carried out to two or more above-mentioned subscriber terminals via the above-mentioned CATV network have (c) central office and the above-mentioned central office (i) A means for receiving the above-mentioned program request code and a means for deciphering the (ii) above-mentioned program request code and determining the above-mentioned program identification code and the above-mentioned terminal identification code from there (iii) A means for answering attestation of a means for attesting the validity of a program determined [ above-mentioned ] and a terminal identification code and the validity of a program by which the (iv) above-mentioned decision was made and a terminal identification code and generating the above-mentioned password.

[Claim 18] The system comprising according to claim 17:

An automatic touch-tone signal detection circuit for detecting each digit of the above-mentioned program request code which a means for [ in the above-mentioned central office / above-mentioned ] receiving was connected to a telephone line and was inputted by member via the above-mentioned telephone line. An audio response unit for being impressed by the above-mentioned telephone line in order to generate in a resultant an audio signal with which the above-mentioned password was sound-ized and for the above-mentioned member to receive the audio signal concerned.

[Claim 19] With an operator of different cable television the above-mentioned system is provided with two or more central offices and each above-mentioned central office is operated and all the operators of the above-mentioned cable

television. Although receiving two or more cryptographic keys of all that distribute two or more programs on the same network to a group of two or more subscriber terminals and can be set to two or more above-mentioned subscriber terminals from the one same operator of cable television is permitted. The different system according to claim 17 from two or more cryptographic keys which can set receiving from an operator of other cable televisions to two or more subscriber terminals to which the permission was granted.

[Claim 20] Cable television comprising:

It is cable television and cable television is (a) cable television distribution network.

(b) A broadcasting organization device of two or more cable televisions formed so that receiving only from each broadcasting organization device might transmit a program via the above-mentioned network defined for two or more permitted subscriber terminals.

(c) Have two or more subscriber terminals connected with the above-mentioned network and each above-mentioned subscriber terminal. A means for obtaining an enciphered event request code which each above-mentioned code is only was provided in (d) above-mentioned each terminal to a certain specific broadcasting organization chose one program including a cryptographic key and was obtained from the above-mentioned cryptographic key.

(e) A means for being provided in two or more above-mentioned broadcasting organization devices being only and generating a password which is only to each specific broadcasting organization to one event. (f) A means for forbidding expressing two or more programs which impressed the above-mentioned password to one terminal in which one program was chosen. controlled a display of a selected program by a terminal in which the above-mentioned program was chosen and were broadcast by this by other broadcasting organizations as other terminals.

[Claim 21] Cable television comprising:

A network.

Two or more subscriber terminals in which receiving two or more signals provided by a specific operator of the operators which were connected with the above-mentioned network and are different was permitted.

A means for limiting reception by two or more above-mentioned members of two or more above-mentioned signals to reception by two or more above-mentioned members of two or more above-mentioned signals provided by a specific operator of two or more above-mentioned operators with which the permission was granted to two or more above-mentioned subscriber terminals.

[Claim 22] With a password for descrambling two or more above-mentioned programs a means for [above-mentioned] limiting is the enabled descrambling code and the above-mentioned password. The system according to claim 21 providing by one specific operator for one invalid specific terminal to another another specific terminal.

[Claim 23] the system according to claim 22 by which also obtaining the above and



the above also acquiring one another specific terminal and receiving two or more signals with one specific operator is characterized by being the permitted terminal.  
[Claim 24] A method characterized by comprising the following for distributing two or more signals to two or more various members.

A described method connects a member of (a) plurality to one program distribution network for receiving two or more programs from a program distribution network.

(b) Connect two or more program feed units to the above-mentioned network.

(c) Download a code related to a certain specific program feed unit to each of two or more various subscriber terminals and store the above-mentioned code in two or more related subscriber terminals.

(d) Two or more programs from two or more above-mentioned program feed units are transmitted to the above-mentioned network by a specific separation channel

(e) Reception of a specific program only from a program feed unit which is related with two or more specific subscriber terminals is enabled using two or more above-mentioned codes.

[Claim 25] A method according to claim 24 including distributing two or more above-mentioned signals via an artificial satellite transmitter.

[Claim 26] A method according to claim 24 including distributing two or more above-mentioned signals via a local transmitter.

[Claim 27] A method according to claim 24 including distributing two or more above-mentioned signals via an optical fiber network of wide area.

[Claim 28] A method characterized by comprising the following for distributing two or more signals to two or more effective members by whom it was connected to a network.

Based on a program sales promotion code a program is required from a program feed unit.

One terminal connected to the above-mentioned network.

A password which is only is supplied to the above-mentioned program.

The above-mentioned password is impressed to the above-mentioned terminal and a program chosen [ above-mentioned ] is executed.

[Claim 29] A method characterized by comprising the following for distributing two or more signals to two or more effective members by whom it was connected to a network.

A program from a program feed unit which supplies a program on a pay-per-view server based on a program sales promotion code is required.

One terminal connected to the above-mentioned network.

A password which is only is supplied to the above-mentioned pay-per-view server.

The above-mentioned password is impressed to the above-mentioned terminal and a program chosen [ above-mentioned ] is executed.

[Claim 30] A method according to claim 29 wherein the above-mentioned password is only to the above-mentioned program again.

[Claim 31] It is a method characterized by comprising the following for distributing two or more signals to two or more effective members and is (a) central office.

Two or more effective subscriber terminal identification codes are stored.

(b) Each broadcasts sales promotion of two or more available services to two or more members in relation to a specific sales promotion code.

(c) Choose one of two or more above-mentioned services and input a selected retailing-of-services promotion code into a terminal in a member's location.

(d) Answer an input of a sales promotion code chosen [ above-mentioned ] and read automatically an identification number relevant to the above-mentioned terminal.

(e) Process a sales promotion code chosen [ above-mentioned ] with the above-mentioned identification number and generate an event request code from there.

(f) Provide an authentication center with the above-mentioned event request code.

(g) A sales promotion code which the above-mentioned event request code was processed accessed the above-mentioned subscriber terminal identification code in the above-mentioned authentication center and was chosen [ above-mentioned ] with the above-mentioned terminal is provided with a password which is only (h)

Provide the above-mentioned member with access to service which answers entering the above-mentioned password into a terminal in the above-mentioned member's location and an input of the (i) above-mentioned password and uses one of two or more of the signals corresponding to a sales promotion code chosen [ above-mentioned ] distributed [ above-mentioned ].

[Claim 32] It is a method characterized by comprising the following for distributing two or more signals to two or more effective members and is the (a) subscriber terminal.

A program code related to service.

A request code for service which uses two or more above-mentioned signals by accessing an address code related to discernment of the above-mentioned terminal is generated two or more above-mentioned codes are processed and a service request code is generated.

(b) Require the above-mentioned service from a central terminal by providing the above-mentioned service request code.

(c) In the above-mentioned central terminal process the above-mentioned service request code check the validity of the above-mentioned address code and the above-mentioned program code and generate a password.

(d) Enter the above-mentioned password into the above-mentioned subscriber terminal answer providing access to two or more above-mentioned signals and provide the above-mentioned service.

[Claim 33] A method according to claim 32 wherein the above-mentioned program code is only to one server of the above-mentioned service.

[Claim 34] A method according to claim 33 wherein the above-mentioned service is offer of a pay-per-view program signal.

[Claim 35]Cable television comprising:

A means to be cable televisionfor the above-mentioned cable television to be provided with a subscriber terminal of (a) pluralityand for each above-mentioned subscriber terminal store a (i) terminal identification code.

(ii) A means for storing a program identification code.

(iii) A means for processing two or more above-mentioned codesand generating a program request code by it.

(iv) A display for displaying two or more programs and displaying the above-mentioned program request code(v) A means for inputting into the above-

mentioned displayin order to receive a passwordto answer this and to display a program on a display(b) It has a head end and a CATV network connected to the

above-mentioned head endThe above-mentioned head end transmits the above-mentioned program to two or more above-mentioned subscriber terminals via the above-mentioned CATV networkhave (c) central officeand the above-mentioned central office(i) A means for receiving the above-mentioned program request code

and determining the above-mentioned program identification code and the above-mentioned terminal identification code from there(ii) A means for answering attestation of validity with a means for attesting the validity of a program

determined [ above-mentioned ] and a terminal identification codeand a program by which the (iii) above-mentioned decision was made and a terminal identification

codeand generating the above-mentioned password.

[Claim 36]Cable television comprising:

It is cable television and the above-mentioned cable television is (a) cable television distribution network.

(b) A broadcasting organization device of two or more cable televisions formed so that receiving only from each broadcasting organization device might transmit two or more programs via the above-mentioned network defined for two or more permitted subscriber terminals.

(c) Have two or more subscriber terminals connected with the above-mentioned networkand each above-mentioned subscriber terminalA means for obtaining an event request code which each above-mentioned code is onlywas provided at (d) above-mentioned each terminal to a certain specific broadcasting organizationchose one program including the 1st codeand was obtained from the 1st key of the above.

(e) A means for being provided in two or more above-mentioned broadcasting organization devicesbeing only and generating a password which is only to each specific broadcasting organization to one event(f) A means for forbidding expressing two or more programs which impressed the above-mentioned password to one terminal in which one program was chosencontrolled a display of a selected program by a terminal in which the above-mentioned program was chosenand were broadcast by this by other broadcasting organizations as other terminals.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to the method concerned and CATV system which are especially used for the effective member of cable (cable) television systems (henceforth a CATV system) useful in a television pay-per-view system about the method and CATV system for distributing a signal.

[0002]

[Description of the Prior Art] Generally charged television systems can be classified into one of the following two ATEGORI.

(a) when paying the monthly contract fee for viewing and listening to all the signals transmitted in the channel between time a member to be (b) When it is viewed and listened by a certain member who pays the fee for the program which the selected program each required namely a member performs pay-per-view (pay per view).

That is according to the number of the programs (program) to which pay per view viewed and listened a member pays a fee. In the 1st category of the above a filter device is removed from the transmission line of the member to whom viewing and listening was permitted or a descrambling signal downloads from a head end to the decoder in a subscriber terminal. In the 2nd category of the above the decoded signal which resembled the specific program and was limited to it by receiving is transmitted to the decoder addressed via the cable network via the telephone line.

[0003] When a member does the member contract of service in each time or when the service concerned is canceled Or it is dramatically expensive to dispatch a serviceman in order to remove or add a filter device on each member's location in the area of much population in each part when the payment for the service concerned is neglected. In order to provide the code (henceforth a descrambling code) for descrambling between the specific time for a specific program It has turned out that the necessary condition for addressing each subscriber terminal with each address is a system smaller than a desired system. Because it is because it is a low speed since the bandwidth which runs short is used and download of a code is needed over long time.

[0004] Such a system was not able to be used using the common cable television network used by the company of two or more cable televisions. Because although the signal with which a right was not given to the member when one member to the company of one cable television telephoned the company of another cable television and got download of the code of descrambling is receivable It is because the profit from [ from the company of the 1st cable television ] the member concerned is snatched.

[0005] Such a system is not suitable to the use for providing other services other than services of original cable televisions such as banking service personal services or order service of goods for example for comparatively poor security. In this case to display the information about fee collections such as a fee collection

statement on a member's television display device is wished.

[0006] The purpose of this invention solves the above technical problem and receives one terminal from one head end on the basis of a terminal A descrambling code or the code for enabling a subscriber terminal. (it is hereafter called an enabling code.) -- downloading [ need and ] . A purveyor of service can make it possible to provide service of an order of banking and goods memory search of personal information etc. for example and can use. It is in providing the effective member of the CATV system for providing service equivalent to pay-per-view or it with the method and CATV system for distributing a signal.

[0007]

[Means for Solving the Problem] A method for distributing two or more signals according to claim 1 concerning this invention to two or more effective members (a) Memorize two or more effective subscriber terminal identification codes in the central office (b) Each broadcasts sales promotion of two or more available services to two or more members connected with a specific sales promotion code (c) Make a sales promotion code of service which chose one of the above-mentioned services of two or more and was chosen input into one terminal in a member's location (d) Answer an input of a sales promotion code chosen [ above-mentioned ] and read automatically an identification number relevant to the above-mentioned terminal (e) Generate an event request code which processed a sales promotion code chosen [ above-mentioned ] with the above-mentioned identification number according to an encryption algorithm and was enciphered from there (f) In supplying the above-mentioned event request code to an authentication center and the (g) above-mentioned authentication center Supplying a password which is only to a sales promotion code which deciphered the above-mentioned event request code and was chosen [ above-mentioned ] with the above-mentioned terminal making the (h) above-mentioned password entering into a terminal in the above-mentioned member's location and an input of the (i) above-mentioned password are answered. It includes providing the above-mentioned terminal with access to one service using one of two or more of the distributed signals corresponding to a sales promotion code chosen [ above-mentioned ].

[0008] A method according to claim 2 includes distributing two or more above-mentioned services by a cable network to two or more above-mentioned members in a method according to claim 1.

[0009] a group of ROM [ in / as for a method according to claim 3 the above-mentioned identification number is fixed in a method according to claim 1 and / each above-mentioned terminal ] and a switch -- it was stored in one

[0010] As for a method according to claim 4 the above-mentioned identification number can change in a method according to claim 2. It is stored in RAM and the above-mentioned identification number is received via a cable addressed by member identified by an address fixed [ above-mentioned ] including further a fixed address relevant to each above-mentioned terminal.

[0011] this invention -- a method according to claim 5 is characterized by that a

method according to claim 2 comprises:

A cryptographic key is transmitted to each of two or more above-mentioned terminals.

The above-mentioned cryptographic key is stored at each above-mentioned terminal.

[0012]A method according to claim 6 is [ this invention ] characterized by that a method according to claim 2 comprises the following again.

Each above-mentioned terminal has the fixed address and a described method transmits two or more cryptographic keys to two or more above-mentioned terminals identified by an address fixed [ above-mentioned ].

The present cryptographic key is stored at each above-mentioned terminal.

[0013]What a method according to claim 7 transmits two or more program codes related to two or more above-mentioned sales promotion codes to each of two or more above-mentioned terminals for in a method according to claim 5It includes deciphering a program code and a terminal identification code as the above-mentioned sales promotion code using a stored cryptographic key and coding and generating the above-mentioned event request code.

[0014]A method according to claim 8 is stored in ROM [ in / in an identification number each fixed / above-mentioned / each above-mentioned terminal ] in a method according to claim 6.

[0015]A method according to claim 9 is characterized by at least one of two or more above-mentioned services being a pay-per-view television signal in a method according to claim 7.

[0016]A step to which the scramble of the above-mentioned television signal is carried out in a method according to claim 9 and which a method according to claim 10 provides with the above-mentioned access includes descrambling the above-mentioned signal at the time of an input of the above-mentioned password.

[0017]A method for this invention to distribute two or more signals according to claim 11 concerning this invention to two or more effective members is characterized by that the (a) subscriber terminal comprises:

A stored program code related to service.

A request code for service which uses two or more above-mentioned signals by accessing an address code related to discernment of the above-mentioned terminal is generated and two or more above-mentioned codes are enciphered using a terminal cryptographic key and a service request code is generated.

(b) Require the above-mentioned service from a central terminal by providing the above-mentioned service request code.

(c) In the above-mentioned central terminal decipher the above-mentioned service request code and check the validity of the above-mentioned address code and the above-mentioned program code and one password is generated (d) Enter the above-mentioned password into the above-mentioned subscriber terminal answer providing access to two or more above-mentioned signals and provide the above-

mentioned service.

[0018]A method according to claim 12 includes downloading a cryptographic key from a head end to the above-mentioned subscriber terminal in a method according to claim 11.

[0019]A method according to claim 13 downloads a cable distributor or two or more operator cryptographic keys in a method according to claim 12 to two or more subscriber terminals from which each subscriber terminal was discriminated by a terminal address.

[0020]In a method according to claim 13 a method according to claim 14Two or more members registered into a broadcasting organization from whom a cryptographic key which changed including supplying two or more above-mentioned signals and downloading the same cryptographic key to all the members registered into each broadcasting organization with two or more broadcasting organizations differed are supplied.

[0021]It is distributed via a cable network where a method according to claim 15 was used in common by broadcasting organization of all the above-mentioned plurality [ signals / above-mentioned / two or more ] in a method according to claim 14.

[0022]In a method according to claim 11since the above-mentioned request code notices about a membra method according to claim 16 is displayed on a screen of televisionand the above-mentioned service is required.

[0023]The cable television according to claim 17 which this invention requires for this invention(a) Have two or more subscriber terminals and each above-mentioned subscriber terminal(i) A means for storing a means and a (ii) program identification codesince a terminal identification code is stored(iii) A means for storing a cryptographic keyand by processing a code and the above-mentioned key of the above-mentioned plurality according to a (iv) encryption algorithmA display for displaying a means for generating a program request codeand a program of (v) pluralityand displaying the above-mentioned program request codeReceive one passwordin order to display a program which should answer it and should be passed on the above-mentioned displayhave a means for inputting into the above-mentioned displayand (vi) The (b) head endIt has a CATV network connected to the above-mentioned head endand is characterized by the above-mentioned head end comprising the following.

A means to transmit a signal with which the scramble of the above-mentioned program was carried out to two or more above-mentioned subscriber terminals via the above-mentioned CATV networkhave (c) central officeand for the above-mentioned central office receive the (i) above-mentioned program request code.

(ii) A means for deciphering the above-mentioned program request code and determining the above-mentioned program identification code and the above-mentioned terminal identification code from there.

(iii) A means for attesting the validity of a program determined [ above-mentioned ] and a terminal identification code.

(iv) A means for answering attestation of the validity of a program determined [ above-mentioned ] and a terminal identification code and generating the above-mentioned password.

[0024] The system according to claim 18 is [ this invention ] characterized by that the system according to claim 17 comprises the following again.

An automatic touch-tone signal detection circuit for detecting each digit of the above-mentioned program request code which a means for [ in the above-mentioned central office / above-mentioned ] receiving was connected to a telephone line and was inputted by member via the above-mentioned telephone line. An audio response unit for being impressed by the above-mentioned telephone line in order to generate in a resultant an audio signal with which the above-mentioned password was sound-ized and for the above-mentioned member to receive the audio signal concerned.

[0025] In the system according to claim 17 the system according to claim 19 the above-mentioned system With an operator of different cable television have two or more central offices and each above-mentioned central office is operated and all the operators of the above-mentioned cable television. Although receiving two or more cryptographic keys of all that distribute two or more programs on the same network to a group of two or more subscriber terminals and can be set to two or more above-mentioned subscriber terminals from the one same operator of cable television is permitted. It differs from two or more cryptographic keys which can set receiving from an operator of other cable televisions to two or more subscriber terminals to which the permission was granted.

[0026] The cable television according to claim 20 concerning this invention (a) A cable television distribution network (b) A broadcasting organization device of two or more cable televisions formed so that receiving only from each broadcasting organization device might transmit a program via the above-mentioned network defined for two or more permitted subscriber terminals (c) Have two or more subscriber terminals connected with the above-mentioned network and each above-mentioned subscriber terminal A means for obtaining an enciphered event request code which each above-mentioned code is only was provided in (d) above-mentioned each terminal to a certain specific broadcasting organization chose one program including a cryptographic key and was obtained from the above-mentioned cryptographic key (e) A means for being provided in two or more above-mentioned broadcasting organization devices being only and generating a password which is only to each specific broadcasting organization to one event (f) Impress the above-mentioned password to one terminal in which one program was chosen control a display of a selected program by a terminal in which the above-mentioned program was chosen and at it by this. It had a means for forbidding expressing two or more programs broadcast by other broadcasting organizations as other terminals.

[0027] This invention is characterized by the cable television according to claim 21 comprising the following.



Network.

Two or more subscriber terminals in which receiving two or more signals provided by a specific operator of the operators which were connected with the above-mentioned network and are different was permitted.

A means for limiting reception by two or more above-mentioned members of two or more above-mentioned signals to reception by two or more above-mentioned members of two or more above-mentioned signals provided by a specific operator of two or more above-mentioned operators with which the permission was granted to two or more above-mentioned subscriber terminals.

[0028]A means for the system according to claim 22 to carry out the above-mentioned limitation in the system according to claim 21With a password for descrambling two or more above-mentioned programsare the enabled descrambling code and the above-mentioned passwordIt is provided by one specific operator for one invalid specific terminal to another another specific terminal.

[0029]the above also obtaining the system according to claim 23 in the system according to claim 22and the above also acquiring one another specific terminaland receiving two or more signals with one specific operator is characterized by being the permitted terminal.

[0030]This invention is characterized by a method comprising the followingin order to distribute two or more signals according to claim 24 concerning this invention to two or more various members.

- (a) Connect two or more members to one program distribution network for receiving two or more programs from a program distribution network.
- (b) Connect two or more program feed units to the above-mentioned network.
- (c) Download a code related to a certain specific program feed unit to each of two or more various subscriber terminalsand store the above-mentioned code in two or more related subscriber terminals.
- (d) Two or more programs from two or more above-mentioned program feed units are transmitted to the above-mentioned network by a specific separation channel(e) Reception of a specific program only from a program feed unit which is related with two or more specific subscriber terminals is enabled using two or more above-mentioned codes.

[0031]A method according to claim 25 includes distributing two or more above-mentioned signals via an artificial satellite transmitter in a method according to claim 24.

[0032]A method according to claim 26 includes distributing two or more above-mentioned signals via a local transmitter in a method according to claim 24.

[0033]A method according to claim 27 includes distributing two or more above-mentioned signals via an optical fiber network of wide area in a method according to claim 24.

[0034]This invention is characterized by a method comprising the followingin order

to distribute two or more signals according to claim 28 concerning this invention to two or more effective members by whom it was connected to a network. Based on a program sales promotion code a program is required from a program feed unit.

One terminal connected to the above-mentioned network.

A password which is only is supplied to the above-mentioned program.

The above-mentioned password is impressed to the above-mentioned terminal and a program chosen [ above-mentioned ] is executed.

[0035] This invention is characterized by a method comprising the following in order to distribute two or more signals according to claim 29 concerning this invention to two or more effective members by whom it was connected to a network.

A program from a program feed unit which supplies a program on a pay-per-view server based on a program sales promotion code is required.

One terminal connected to the above-mentioned network.

A password which is only is supplied to the above-mentioned pay-per-view server.

The above-mentioned password is impressed to the above-mentioned terminal and a program chosen [ above-mentioned ] is executed.

[0036] A method according to claim 30 is characterized by the above-mentioned password being only to the above-mentioned program again in a method according to claim 29.

[0037] A method for distributing two or more signals according to claim 31 concerning this invention to two or more effective members (a) Store two or more effective subscriber terminal identification codes in the central office (b) Each broadcasts sales promotion of two or more available services to two or more members in relation to a specific sales promotion code (c) Choose one of two or more above-mentioned services and input a selected retailing-of-services promotion code into a terminal in a member's location (d) Answer an input of a sales promotion code chosen [ above-mentioned ] and read automatically an identification number relevant to the above-mentioned terminal (e) In processing a sales promotion code chosen [ above-mentioned ] with the above-mentioned identification number and generating an event request code from there providing an authentication center with the (f) above-mentioned event request code and the (g) above-mentioned authentication center A sales promotion code which the above-mentioned event request code was processed accessed the above-mentioned subscriber terminal identification code and was chosen [ above-mentioned ] with the above-mentioned terminal is provided with a password which is only (h) Answer entering the above-mentioned password into a terminal in the above-mentioned member's location and an input of the (i) above-mentioned password It includes providing the above-mentioned member with access to service using one of two or more of the signals corresponding to a sales promotion code chosen [ above-mentioned ] distributed [ above-mentioned ].

[0038] A method for this invention to distribute two or more signals according to

claim 32 concerning this invention to two or more effective members is characterized by that the (a) subscriber terminal comprises:

A program code related to service.

A request code for service which uses two or more above-mentioned signals by accessing an address code related to discernment of the above-mentioned terminal is generated two or more above-mentioned codes are processed and a service request code is generated.

(b) Require the above-mentioned service from a central terminal by providing the above-mentioned service request code.

(c) In the above-mentioned central terminal process the above-mentioned service request code check the validity of the above-mentioned address code and the above-mentioned program code and a password is generated (d) Enter the above-mentioned password into the above-mentioned subscriber terminal answer providing access to two or more above-mentioned signals and provide the above-mentioned service.

[0039] A method according to claim 33 is characterized by the above-mentioned program code being only to one server of the above-mentioned service in a method according to claim 32.

[0040] A method according to claim 34 is characterized by the above-mentioned service being offer of a pay-per-view program signal in a method according to claim 33.

[0041] The cable television according to claim 35 which this invention requires for this invention (a) Have two or more subscriber terminals and each above-mentioned subscriber terminal (i) A means for storing a means and a (ii) program identification codes since a terminal identification code is stored (iii) A means for processing two or more above-mentioned codes and generating a program request code by it (iv) A display for displaying two or more programs and displaying the above-mentioned program request code (v) A means for inputting into the above-mentioned display in order to receive a password to answer this and to display a program on a display (b) It has a head end and a CATV network connected to the above-mentioned head end and the above-mentioned head end transmits the above-mentioned program to two or more above-mentioned subscriber terminals via the above-mentioned CATV network and it has (c) central office and is characterized by the above-mentioned central office comprising the following.

(i) A means for receiving the above-mentioned program request code and determining the above-mentioned program identification code and the above-mentioned terminal identification code from there.

(ii) A means for attesting the validity of a program determined [ above-mentioned ] and a terminal identification code.

(iii) A means for answering attestation of validity with a program determined [ above-mentioned ] and a terminal identification code and generating the above-mentioned password.

[0042]The cable television according to claim 36 concerning this invention(a) A cable television distribution network(b) A broadcasting organization device of two or more cable televisions formed so that receiving only from each broadcasting organization device might transmit two or more programs via the above-mentioned network defined for two or more permitted subscriber terminals(c) Have two or more subscriber terminals connected with the above-mentioned networkand each above-mentioned subscriber terminalA means for obtaining an event request code which each above-mentioned code is onlywas provided at (d) above-mentioned each terminal to a certain specific broadcasting organizationchose one program including the 1st codeand was obtained from the 1st key of the above(e) A means for being provided in two or more above-mentioned broadcasting organization devicesbeing only and generating a password which is only to each specific broadcasting organization to one event(f) Impress the above-mentioned password to one terminal in which one program was chosencontrol a display of a selected program by a terminal in which the above-mentioned program was chosenand at it by this. It had a means for forbidding expressing two or more programs broadcast by other broadcasting organizations as other terminals.

[0043]

[Function]According to this inventionone terminal is received from one head end on the basis of a terminalIt does not need to download an enabling code for a descrambling code or a subscriber terminal. A purveyor of service can make it possible to provide service of an order of banking and goodsmemory search of personal informationetc.for exampleand can use. The effective member of the CATV system for providing service equivalent to pay-per-view or it is provided with the method and CATV system for distributing a signal.

[0044]the system concerned says that another cable television with one another member of one cable television to a program or service can place an order -- dangerous -- to carry outWith the operator of two or more cable televisionsuse of one network can be made easy.

[0045]Although it is not necessary to necessarily link to the distribution system of a cable networkthe system concerned can be used in order to control offer of a useful signal to the member distributed by the broadcasting organization "under broadcast"the satellite broadcasting entrepreneuretc. [ local ]

[0046]The system concerned without the necessity for the head end for transmitting to the terminal which had the specific enabling code or especially the descrambling code addressed again for exampleIt makes it possible for two or more members permitted especially to choose dataor to receive dataIn order to make it possible to change the data concerned into a reporta messagea newspaperthe statement (a declaration or a public notice) of a bankthe slip (check) of a checketc. via the facsimile machine equipped in order to receive a signalUsing is appropriate in order "to broadcast to a specific area (narrowcast)."

[0047]When a member enters one password to a terminaleach terminal can be separately enabledin order to receive the signal of the sequence demanded especially which directs a programserviceetc. (operation is possible). Typicallythe

password concerned is entered by push button type (touch tone (registered trademark)) telephone and is obtained from the central office which attested the event request code which provides the above-mentioned password by a synthetic-voice-response system. After the event request code concerned inputs the demand to a specific program or service with a member into the terminal concerned it is supplied on the television screen of the member concerned.

[0048] In a certain pay-per-view system a barker (tout) channel displays an available program and service with a number respectively. A corresponding number is inputted into a subscriber terminal by the member when asking for a certain specific program or service. In the interval the subscriber terminal stores various programs and the identification code of service in one memory.

In order to confirm whether the input error arose the number inputted by the member is checked with reference to the number stored [ above-mentioned ].

[0049] Subsequently a subscriber terminal searches the only logical or physical terminal address (I. D. : an identification address or terminal ID) storable in ROM a DIP switch etc. the program or service identification code corresponding to the program or service chosen [ above-mentioned ] [ search and ] The enciphered event request code which processes a program number and terminal ID using the algorithm using the cryptographic key concerned and is displayed on a television screen is generated using a cryptographic key. In the desirable mode concerning this invention although the code has the length of 14 digits including an arithmetic check number other code length can be used according to the necessity for the company of not only this but cable television. Subsequently a member initializes action which places an order for a pay-per-view event. Supposing it is wanted the automatic number discernment (ANI: Automatic Number Identification) which can decrease the number of digits used may be used.

[0050] In order to place an order the event request code displayed to the member on the television screen is provided by the telephone to the central office by a member. The above-mentioned central office provides an above-mentioned password by the response of the sound which deciphered the code checked the terminal number with reference to the list of effective subscriber terminal numbers and checked the above-mentioned program code for example was generated to the member at the resultant. Subsequently a member enters the password concerned into a terminal and here the password concerned it not only provides a specific descrambling code but it receives a terminal to an event a program service etc. which were demanded from the terminal. At the time of a certain program and attest the terminal for descrambling between the time when the above-mentioned descrambling code is outputted and preferably in during the specific time when it has been a certain specific time to the above-mentioned terminal. The command for switching the output to a television display to the demanded channel which may be a barker channel automatically is provided and a program is automatically provided by this to a member.

[0051] Once a member is provided with a password accounting of the order to a

pay-per-view event will be received and carried outnamely a bill will be filled in and a bill will be published. A member has an option for canceling order completion to the start of the event concerned. Processing of cancellation is the same as processing of a demand of an event. The program chosen [ above-mentioned ] is displayed as a list on a television screen when you choose the "cancellation" option in a barker menu. Once it can choose so that you may cancel a program and it is performed the cancellation code of 14 digits will be displayed and the above-mentioned program will be immediately canceled in the terminal concerned. The code of the 14 above-mentioned digit is given to a head end and before a program begins it needs to cancel a bill. After obtaining the cancellation code enciphered on the above-mentioned television screen a member transmits the cancellation code concerned to the central office using a different telephone number from the telephone number used in order to place an order. A different password is given to a member and in order to carry out completion execution of the processing of the cancellation concerned it is entered into a terminal.

[0052] It is impossible to decipher the enciphered code which was generated using encoding technology in recent years in within a time [ which provides security substantially / rational ] as a matter of fact. The cryptographic key stored in various terminals can sometimes be changed by what (or it transmits widely) is broadcast from a head end every two months to the terminal in which each was addressed with the permanent address of the terminal concerned for example. In this case each terminal does not need to be addressed just before the selected program or service but it is clear its to save the sending set needed in peak time etc. and bandwidth.

[0053] Since two or more codes in relation to various programs can be chosen by the supplier of cable television service typically From transmission of a pay-per-view program several hours ago it is not simply provided to the Barker channel even one day or two days ago but both the codes and passwords which were enciphered. In order to make it possible to descramble the distributed pay-per-view signal not only depending on a cryptographic key but depending on a program number and to use it by fraudulent practice it is impossible to generate a suitable password by an illegal furtive glance listener within predetermined time as a matter of fact.

[0054] The cryptographic key needs to be cautious of the ability to be made to differ to each of the operator of some cable televisions which distribute two or more signals on the same cable television network or other media. Therefore the subscriber terminal relevant to the operator of the cable television in which the member did the participating contract which has the stored specific cryptographic key The event request code which is not recognized by the central office device of the operator of another cable television will be generated the demand by one member of the operator of another cable television is answered and neither the password nor the effective password will be generated. This provides a member's separation in order that the operator of all the cable televisions may separate the operator of the cable television of these plurality connected to one network. Therefore the field of a certain whole is among [ network ] one or within one group

[ one ] of a network to some extent one equipment is provided so that it can be connected. Two or more members' monopoly or exclusive rights does not exist to one operator but two or more members can choose the operator of one of the cable televisions for which it asks. The operator of two or more cable televisions served to the residents who overlap does not have to double one cable television network therefore can save remarkable expense.

[0055] According to one mode concerning this invention the method of distributing two or more signals to two or more effective members In the central office the effective identification code of at least one subscriber terminal is stored Each broadcasts sales promotion of two or more available services to two or more members connected with a specific sales promotion code The sales promotion code of the service which chose one of the above-mentioned services of two or more and was chosen is made to input into one terminal in a member's location The input of a sales promotion code chosen [ above-mentioned ] is answered and the identification number relevant to the above-mentioned terminal is read automatically The sales promotion code chosen [ above-mentioned ] with the above-mentioned identification number according to the encryption algorithm is processed In generating the event request code enciphered from there supplying the above-mentioned event request code to an authentication center and an authentication center deciphering the above-mentioned event request code and the above-mentioned number -- the above -- with reference to two or more effective identification codes [ attest and ] The above-mentioned password is made [ supplying the sales promotion code chosen / above-mentioned / with the only password to the above-mentioned terminal and ] to enter into the terminal in the above-mentioned member's location It includes providing the above-mentioned terminal with access to one service using one of two or more of the distributed signals corresponding to the sales promotion code which answered the input of the above-mentioned password and was chosen [ above-mentioned ].

[0056] According to another mode concerning this invention the method for distributing two or more signals to two or more effective members In a subscriber terminal by accessing the stored program code related to service and the address code related to discernment of the above-mentioned terminal The request code for service using two or more above-mentioned signals is generated two or more above-mentioned codes are enciphered using a cryptographic key and a service request code is generated In requiring the service from a central terminal by supplying the above-mentioned service request code and a central terminal The above-mentioned service request code is deciphered the validity of the above-mentioned address code and the above-mentioned program code is checked and one password is generated It includes entering the above-mentioned password into the above-mentioned subscriber terminal and answering offer of access to two or more signals and providing service.

[0057] According to another mode concerning this invention cable television Have two or more subscriber terminals and each above-mentioned subscriber terminal According to the device for storing a terminal identification code the device

for storing a program identification code the device for storing a cryptographic key and an encryption algorithm process the code and the above-mentioned key of the above-mentioned plurality and by this. The device for generating a program request code and the display for displaying two or more programs and displaying a program request code including the device for inputting into the above-mentioned display in order to receive one password to answer it and to display a program on the above-mentioned display a head end have the CATV network connected to the above-mentioned head end and the above-mentioned head end further transmit the signal with which the scramble of the above-mentioned program was carried out to two or more above-mentioned subscriber terminals via the above-mentioned CATV network have the central office and the above-mentioned central office a device for receiving the above-mentioned program request code and a device for deciphering the above-mentioned program request code and determining the above-mentioned program identification code and the above-mentioned terminal identification code from there it has a device for answering attestation with the device for attesting the validity of the program determined [above-mentioned] and a terminal identification code and the program determined [above-mentioned] and the validity of a terminal identification code and generating the above-mentioned password.

[0058] According to another mode concerning this invention cable television a broadcasting organization device of two or more cable televisions formed so that a program might be transmitted via a cable television distribution network and the network defined for two or more subscriber terminals in which receiving only from each broadcasting organization device was permitted having two or more subscriber terminals connected with the above-mentioned network each above-mentioned code of each above-mentioned subscriber terminal is only to a certain specific broadcasting organization including a cryptographic key.

A device for obtaining the enciphered event request code which was provided at each above-mentioned terminal chose one program and was obtained from the above-mentioned cryptographic key a device for being provided in two or more above-mentioned broadcasting organization devices being only and generating the password which is only to each specific broadcasting organization to one event impress the above-mentioned password to one terminal in which one program was chosen control the display of the program selected at the terminal in which the above-mentioned program was chosen and by this. It has a device for forbidding expressing two or more programs broadcast by other broadcasting organizations as other terminals.

[0059] According to another mode concerning this invention cable television two or more subscriber terminals connected to the network with which receiving two or more signals provided by some specific operators of several operators which were connected to one network and the above-mentioned network and are different was permitted it has a device for restricting reception of the signal by two or more above-mentioned members to the signal of the program provided by some specific



operators of two or more operators with which the permission was granted to two or more above-mentioned subscriber terminals.

[0060] According to another mode concerning this invention the method for distributing two or more signals to various members Two or more members are connected to one program distribution network for receiving the program from a network It stores [ connecting two or more program feed units to the above-mentioned network and ] with the subscriber terminal which downloads the code related to a certain specific program feed unit to each of various subscriber terminals and is related to it in the above-mentioned code It includes transmitting two or more programs from two or more above-mentioned program feed units to the above-mentioned network by the separated specific channel and enabling reception of the specific program only from a program feed unit which is related with a specific subscriber terminal using two or more above-mentioned codes.

[0061]

[Example] Hereafter the example which starts this invention with reference to drawings is described. Drawing 1 is a block diagram of the CATV system of one example concerning this invention. Not illustrating since it is publicly known to a person skilled in the art about the structural portion of the television distribution system which is unrelated to this invention will be recognized.

[0062] The head end 1 generates two or more program signals such as two or more CATV signals and transmits them via the media 3. According to the desirable example concerning the successful prototype concerning this invention or this invention the media 3 are cable television distribution networks. However it will be understood that the head end 1 can be transmitted for example via satellite distribution systems such as an optical fiber network (information superhighway) the usual local broadcast and a Wide Area Network (WAN). The signal transmitted by the head end 1 is supporting commercially two or more signals distributed for nothing the television signal by which scramble was carried out or other signals which provide two or more various services to two or more various members. although the following description comes out mainly about two or more signals distributed for nothing it is made about the signal by which scramble was merely carried out. Therefore the component of the subscriber terminal which bypasses a descrambler / converter 7 or provides the input of for example a facsimile port or a computer etc. with two or more signals is not illustrated. However these structural concepts of one terminal are indicated in U.S. Pat. No. 4623920 which was publicly known to the person skilled in the art and was invented by Michel Dufresne (Michel Dufresne) etc. and was given on November 18 1986.

[0063] It is received by the subscriber terminal 5 and two or more signals transmitted from the head end 1 are supplied to the input of a descrambler / converter 7. Supposing the DESURAN bull code was not received by a descrambler / converter 7 What is displayed on the video monitor 9 which two or more signals concerned passed the descrambler / converter 7 and was connected to the output of its descrambler / converter 7 so that an understanding is possible is blocked.

[0064]By two or more members set working and the head end 1 transmits without applying scramble on a barker channel and the display or display for sales promotion of two or more available services here Each of two or more members relates to the related sales promotion (or advertisement) code. Two or more services concerned consist of such a television program including a television program by which to view and listen in a pay-per-view system is wished and by which scramble was carried out. The list is collectable from the pay-per-view service feed unit 2.

[0065]Two different pay-per-view auxiliary channels [ finishing / scramble ] transmitted from the head end 1 at the time which two or more programs which should be chosen as a certain suitable time were transmitted in other channels again for example was decided beforehand may exist.

[0066]The scramble of the barker channel is not carried out but it is whether a descrambler / converter 7 is bypassed or to pass without the necessary condition [ DESURAMBURU / necessary condition ] via a descrambler / converter 7 and is displayed on the video monitor 9 after that. The member concerned views and listens to a barker channel and chooses the programme service identified by one certain program code.

[0067]Subsequently the member concerned inputs the program code concerned into the subscriber terminal 5 by the means of remote control which the encryption processor 11 is made to pass for example.

[0068]One group of two or more DIP switches who the terminal address module 13 relates to the subscriber terminal 5 and identifies the subscriber terminal 5 logically Or they are the logical address memorized by the read only memory (ROM) an address in firmware or the address eternally memorized by some of other methods.

[0069]The subscriber terminal 5 contains the memory 15 which memorizes or stores a cryptographic key again.

[0070]When a member inputs a program code into the subscriber terminal 5 for example for service like a pay-per-view program for which it asked especially An encryption algorithm accesses a cryptographic key from the serial number which discriminates a terminal from the module 13 and the memory 15 and ranks second using a program code above-mentioned data is processed according to the above-mentioned encryption algorithm and the enciphered event request code is generated. In the desirable example of this invention an event request code has the length of 14 digits and the detailed after-mentioned is carried out about this.

[0071]The signal of the program number of two or more services which make a sales promotion on a barker channel needs preferably to be stored in the program memory 17 connected so that these signals might be received from a descrambler / converter 7. Before the processor 11 generates an event request code preferably the processor 11 needs to access the above-mentioned program memory 17 and needs to compare the stored program number with the program code into which it was inputted by the member. If detecting the program code into which the processor 11 was inputted goes wrong Clearly the member is doing the

erroneous input (error) in the input and the processor 11 transmits a certain signal to a descrambler / converter 7 via the path 19. A certain message can be displayed on the video monitor 9 and it can tell that the program code mistaken to the member concerned was inputted.

[0072] It is told to a member that it telephones to the telephone number which was able to determine beforehand the event request code displayed to assume that the program code was attested with the right for example. In order to display to a member using the suitable message generated by the video presentation signal generator 20 connected to the descrambler / converter 7 on the video monitor 9, the event request code generated by the processor 11 is passed by a descrambler / converter 7 via the signal path 19.

[0073] Subsequently a member calls to the central office including the check system 24 which is later mentioned using the member's telephone 21. The event request code enciphered by push button type (touch tone) telephone or a device equivalent to it is inputted and the event request code concerned is transmitted to the telephone 25 and modem which are in the check system 24 of the central office via the telephone line 23 or a device equivalent to them.

[0074] When one command is inputted into the subscriber terminal 5 including a modem, it may be made for the subscriber terminal 5 to dial the above-mentioned modem to the corresponding modem in the central office automatically rather than a member dials using the member's telephone 21. Therefore in such an example, the telephones 21 and 25 need to be transposed to two modems which communicate automatically mutually.

[0075] The format with common 14 digit code in a desirable example: It has the form of AAAAAAEEEECBBBV.

[0076] Here AAAAAA(s) are a number of the decimal numeral of 6 figures of fields taken from the terminal address of the subscriber terminal 5 and are the only identification codes of the subscriber terminal in which an order for an event is placed from there and a program or service is transmitted there.

[0077] EEE is the field including the number of the service ordered by the member or a pay-per-view event. A different event number is assigned to each time provided with each event and the event concerned. For example, to the odd moon, an event number is specified in the ranges from 001 to 399 to a movie and a special event receives and it is specified in the ranges from 400 to 499. To the even moon, an event number is specified in the ranges from 501 to 899 to a movie and a special event receives and it is specified in the ranges from 900 to 999.

[0078] C field contains the logical channel number of the event it is broadcast that the event concerned is. The possible value is in from 0 before 9. In the small system using the above-mentioned format, 0 is an advertisement channel called a barker channel, 1 is the 1st pay-per-view channel and 2 is the 2nd pay-per-view channel for example. Two or more logical channels are changed into two or more specific channels by a descrambler / converter 7. For example, the logical channel 1 is chosen, being decrypted is enabled and the channel 56 can be specified as 1st pay-per-view channel, it is decrypted and can be displayed on the channel 14.

which is the typical Barker channel.

[0079]BBB is the fee collection (bill) code generated by the subscriber terminal 5. A fee collection code is used [ generating the code concerned againwhen a member uses a member's subscriber terminal own / the /and ] in order to receive attestation to a central terminal. The BBB fee collection code concerned is generated using the cryptographic key stored in the read only memory (ROM) in the subscriber terminal 5.

[0080]V is an authentication code calculated from 13 front numbers. It is used in order to show not having carried out the erroneous input (error) at all to a central terminalwhen a user inputs the data for an event.

[0081]When referring to drawing 1 now and an event request code is received by the telephone 25 or the modem equivalent to itthat is detected in the interface 27 of the check system 24. This was checked by reconstructing authentication code V combined with the decryption system 29or I hear that it validated and it has the event request code inputted by the member. If invalid judgment is madein order to ask a member to input againa feedback message is transmitted to a member and the above-mentioned message is a voice message compounded supposing telephone was used here.

Or if a modem is usedit will be a message for displaying on the screen of a member's television.

[0082]In one example of the check system 24the table 33 stores the list of all the effective members' serial numbers in the check system 24 concernedand the table 35 stores the list of programs effective there. The processor 36 reads data from the table 33and it is determined whether one effective terminal address was inputted. The table 35 is checked in order to check that one effective program number has been inputted.

[0083]In another example illustrated in drawing 2the check system 24A detects the validity of an event request codeand is provided with the PPV server 31 which generates the password impressed to the interface 27. The interface 27 is a language of the sound formed in the resultantthe number and/or character of a password which are acoustically reproduced in the telephone 25 are generatedand it is supplied to the member by whom the event request code was inputted by this.

[0084]Instead a password is impressed to an above-mentioned modem and with a local modem and the data receiver 37 in localAfter being changed into the signal which can be recognized by the descrambler / converter 7since it is impressed by the descrambler / converter 7a passage input is directly carried out to the subscriber terminal 5.

[0085]According to another examplethe table 33 is made unnecessary. The enciphered event request code contains a checksum. If right when it is first decided to an event request code that the checksum concerned will be the rightan event request code will be deciphered and it will be determined that one effective member demanded one event. Supposing it is shown as an invalid member

supposing the above-mentioned code is undecipherable or a checksum is not right the error has arisen or interference has arisen on the transmission line. An event is refused at one of cases.

[0086] Supposing a code is deciphered the table 35 will be accessed in order to determine whether one effective program was chosen. Instead the table 35 is not used but assumption that the validity of a program is checked with generation of an event request code with the subscriber terminal 5 is made.

[0087] If it assumes that it is the member who heard the password from the telephone 25 it will rank second and the member will enter a password into the subscriber terminal 5 by inputting a password into the remote control of his terminal for example. It is received by the data receiver 37 the password concerned is changed into the signal which can be recognized by the descrambler / converter 7 and the password concerned is impressed there. After the password concerned is received the encryption processor 11 performs reverse processing and decipheres the password concerned. The result is compared with the request code of the origin currently held at the subscriber station for the check. When not in agreement an invalid message appears on a screen.

[0088] Supposing a password is received the program for which this asked between suitable time and suitable time will be displayed.

[0089] In order to control two or more members' validity the check system 24 of the central office is provided with SMS (service management system) containing the charging device 39 illustrated in detail in drawing 1. As for the charging device 39 it is possible for it to be a personal computer operated by the operator of cable television. It had a good credit history or the fee is beforehand paid to a certain program (.). That is two or more members registered to the operator of the specific cable television which is carrying out prepaid ones are inputted into the charging device 39 which stores the address of two or more terminals of such two or more effective members in the table 33.

[0090] It is necessary to notice the charging device 39 about it being possible for it to be related to the operator of a certain specific cable table. By one DCH a cryptographic key is broadcast to each member ranks second and is memorized by the memory 15 of the subscriber terminal 5. A cryptographic key is preferably changed from the head end 1 for example with time intervals decided beforehand such as two months and one etc. month. A cryptographic key can be generated by the charging device 39 or the network monitor (not shown).

Receiving two or more program and two or more services from the operator of one cable television can be used by one cryptographic key for all the members attested or permitted.

[0091] Several different central offices 24 are able to connect with the head end 1 relevant to the operator of each cable respectively. However all the subscriber terminals 5 can be connected with the media 3 of the same cable television network. In order to separate two or more subscriber terminals connected with the operator of each cable television all the subscriber terminals attested or permitted receiving from the operator of a certain specific cable television need to have the

same cryptographic key. Several different cryptographic keys are used [ receiving from the operator of different cable television and ] with two or more subscriber terminals to which the permission was attested or granted.

[0092]As the above-mentioned result two or more event request codes are not recognized by the central office 24 of the operator of two or more cable televisions related to two or more subscriber terminals attested or permitted to the operator of different cable television. Therefore the operator of two or more cable televisions can use the same network and can pool a free cable channel and transmission of service. It can be held by those pay-per-view customers in the state where it is dissociated as a whole because of several different cryptographic keys. This makes perfect security (security) possible to the operator of various cable televisions which carry out a participating contract to a different supplier of service for each of those systems.

[0093]The more detailed block diagram of the subscriber terminal 5 is illustrated by drawing 4. The input terminal 41 receives the signal from the media 3 and outputs those signals to the converter 43. Typically the converter 43 changes the channel of an input signal into the channel 3 for the display on the video monitor 9 for example. To two or more usual signals since it is impressed by the input video of the video monitor 9 via the switch 45 the passage output of the output of the converter 43 is carried out on the video output line 46.

[0094]The switch 45 can impress the output of the converter 43 to the descrambler 47 instead. The converter 43 the switch 45 and the descrambler 47 are controlled by the microprocessor 49 via the bus 51.

[0095]The receiver 53 by which remote control is carried out receives two or more infrared signals from the transmitter of remote control used by one member for example and changes two or more signals concerned into the signal of a digital format and those signals are impressed to the bus 51 in order for the microprocessor 49 to receive. Random-access-memory RAM 55 stores two or more programs for using it by the microprocessor 49 when performing two or more functions of the subscriber terminal 5. The microprocessor 49 can access the data stored in RAM 55 in order to display on the video monitor 9 and it ranks second After generating a status signal using the video presentation signal generator 56 the signal concerned Digital one/analog converter. (It is hereafter called an A/D converter.) It is impressed by 57 and in A/D converter 57 concerned the above-mentioned signal can be displayed on the video monitor 9 it becomes irregular with the modulator 48 and the signal concerned is impressed to the output line 46.

[0096]The above-mentioned usual operation is indicated in U.S. Pat. No. 4623920 which was invented by Michel Dufrene (Michel Dufresne) etc. and was given on November 18 1986 and this is contained by referring to it here.

[0097]The terminal address module 13 is connected to the bus 51 and the microprocessor 49 can access and read the serial number of the subscriber terminal 5 concerned by this. The code key memory 15 can store the above-mentioned cryptographic key sent from the head end 1.

[0098]The RAM program memory 17 is connected to the bus 51 in order to access

by the microprocessor 49.

[0099]For example two or more programs on the barker channel which is the channel 14 are displayed by bypassing the descrambler 47. The data transmitted on the DCH which can be existed in the vertical interval or the line 21 of a barker channel is impressed via the converter 43 or it gets over with a demodulator (not shown) and is outputted to the bus 51. This data is a program identification number (or program identifier number) relevant to two or more programs listed on the barker channel for example. It controls that the microprocessor 49 stores this data in the program memory 17.

[0100]When a program list is seen by the member on a barker channel the member chooses one program by inputting the program code which is displayed for example using his remote control and is related. In [preferably the program code concerned is given in front by a specific identifier like \* or the specifier character before a number is inputted into the remote-control receiver 53 by the remote control transmitter and ] the receiver 53 concerned The above-mentioned program code is changed into data and is temporarily stored in RAM55. The microprocessor 49 detects a program code and determines the event code which is a digit which serves as EEE referred to above from there for example using one program stored in RAM55. Subsequently the microprocessor 49 checks those digits using the corresponding digit stored in the program memory 17 and supposing it is effective it will access the encryption algorithm stored in RAM55.

[0101]When processing using an encryption algorithm while the microprocessor 49 accesses a serial number from the module 13 The program number which was temporarily stored in RAM55 and which was chosen [above-mentioned] is accessed and the event request code of 14 digits is generated preferably. The microprocessor 49 formulates the above-mentioned event request code in the form which can be displayed using the video presentation signal generator 56 for example adds some characters for explanations such as a report of a check and a command It telephones to a certain telephone number obtained by accessing the data stored in RAM55 and in order to display the information concerned on the above-mentioned video monitor 9 it is impressed by it. Looking at the event request code displayed on the video monitor 9 the above-mentioned member dials the digit of the directed telephone number and as mentioned above he receives a password from the central office 24. Subsequently a member inputs into a terminal remote control the password received by the remote-control receiver 53. The password concerned is temporarily stored in RAM55. The microprocessor 49 decrypts the password concerned using the program stored here to enabling time enabling time a descrambling code and a channel-control signal for the descrambler 47.

[0102]The following things will be understood. It is a basis of control of the microprocessor 49 instead of being able to connect the modem 61 to the bus 51 and an event request code being inputted into telephone by the member Can dial the modem 61 to the modem in the central office 24 it can transmit an event request code to the modem concerned automatically and ranks second A password

is received from there and the password concerned is impressed to the bus 51 for the use which follows the it by storing and the microprocessor 49 in RAM55.

[0103]At the suitable time directed by the clock circuit 59the microprocessor 49The switch 45 is switched so that the output of the converter 43 may be outputted to the input of the descrambler 47The descrambling code stored [ above-mentioned ] is impressed to the descrambler 47It switches so that it may receive from a certain specific channel which was directed by the logical channel to which the tuner contained in the converter 43 was directed in the password and by which scramble was carried outIt crawls on the signal concerned to a barker channel to the converter 43 againand is made to output to the channel of everything but shoes decided beforehand. Thereforethe scramble of the demanded channel is changed and carried outand it is impressed to the output line 46 for the display on the video monitor 9.

[0104]After the time interval the program was instructed to be the microprocessor 49 removes the scramble code 47It makes it possible to display the usual free channel on the video monitor 9 by switching so that it may return to the channel aligned or switched before the converter 43and switching the switch 45 so that the descrambler 47 may be bypassed.

[0105]Supposing it asks for two or more memories explained with reference to the example of drawing 4it will be understood that it is combinable by an efficient method. A backup cell needs preferably to use it in order to hold the data which was stored at the memory in the case of power failure.

[0106]Drawing 5 is a block diagram illustrating the network of two or more operators. The operator control systems (henceforth an operator system) 70A thru/or 70N of two or more cable televisionsrespectivelyTwo or more programs are transmitted to the group of the member of itself via the common network 72and each of these members' group is connected to the same common network. Each member has the reception-control subscriber terminal which was explained with reference to drawing 4. Each member receives two or more signals from a main head and 72 by other means for cable link and microwave linking 74 or receiving two or more signals. The operator system of each cable television is provided with the program permission and the authentication system which consist of a member of itselfand SMS(service management system) 30A thru/or 30N and the servers 31A thru/or 31N. Each program permission and an authentication system have a telephone number of itself for the telephone line 25. Thereforethe operator system of each cable televisionThe subscriber terminal for the member of the group of itself and two or more decryption codes can be providedTwo or more program codes of itself can be provided on the Barker channel of itselfand it can attest or permit receiving two or more programs by providing the password of itself to two or more members of itself. It will be recognized about the operator of each cable television operating SMS30 and the server 31 instead of it that the operator of the head end 72 and the contract of a contract can be performed. Since it is establishednot using the code in which the operator of each cable television has interfered mutually (Inta fair) or which it overlaps preferablyThe



operator of the head end 72 needs to assign the only code separately to each of two or more operator systems. Two or more operator systems operate within the common network 72as mentioned above. When using each of various terminals which stores the peculiar only common code to the operator system of a certain specific cable televisionEven if it is a case where it is not pay-per-view program supplyreception of the program by each of two or more subscriber terminals can be limited to the program sent out by the operator system of related cable television. It is because the code can control the scramble processing of the usual program signal transmitted with the only scramble code by each of various operator systems. In order to be able to receive other programs from the head end 72and not to carry out scramble by the operator system of the above-mentioned cable television but to see without a limited condition generally by all the membersIt is transmitted in common by the operator system of all the cable televisions. Although the above-mentioned network does not need to be a CATV systemthey may be the arbitrary forms of the program distribution system of many viewers who transmit the signal of the forms that it is arbitrary for reception by many viewers.

[0107]Those who understand this invention may consider the structure of modificationan exampleor the above-mentioned modification. I think that all it is a part of this inventions which are contained in the claim of attachment on these specifications.

[0108]

[Effect of the Invention]As explained in full detail aboveit is the method of distributing two or more signals to an effective member according to this inventionand the effective identification code of a subscriber terminal is memorized in (a) central office(b) Each broadcasts sales promotion of two or more available services to two or more members connected with a specific sales promotion code(c) Make the sales promotion code of the service which chose one of the above-mentioned services of two or moreand was chosen input into one terminal in a member's location(d) Answer the input of a sales promotion code chosen [ above-mentioned ]and read automatically the identification number relevant to the above-mentioned terminal(e) Generate the event request code which processed the sales promotion code chosen [ above-mentioned ] with the above-mentioned identification number according to the encryption algorithmand was enciphered from there(f) In supplying the above-mentioned event request code to an authentication centerand the (g) above-mentioned authentication centerSupplying the password which is only to the sales promotion code which deciphered the above-mentioned event request codeand was chosen [ above-mentioned ] with the above-mentioned terminalmaking the (h) above-mentioned password entering into the terminal in the above-mentioned member's locationand the input of the (i) above-mentioned password are answeredIt includes providing the above-mentioned terminal with access to one service using one of two or more of the distributed signals corresponding to the sales promotion code chosen [ above-mentioned ].

[0109]Therefore one terminal is received from one head end on the basis of a terminal. It does not need to download an enabling code for a descrambling code or a subscriber terminal. A purveyor of service can make it possible to provide service of an order of banking and goods memory search of personal information etc. for example and can use. The effective member of the CATV system for providing service equivalent to pay-per-view or it can be provided with the method and CATV system for distributing a signal.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] It is a block diagram of the CATV system which is one example concerning this invention.

[Drawing 2] It is a block diagram of the modification of the check system in drawing 1.

[Drawing 3] It is a block diagram of another modification of the check system in drawing 1.

[Drawing 4] They are some block diagrams of the subscriber terminal in drawing 1.

[Drawing 5] It is a block diagram of the program broadcasting system of two or more operators.

[Description of Notations]

- 1 -- Head end
- 2 -- PPV (pay-per-view) service feed unit
- 3 -- Media
- 5 -- Subscriber terminal
- 7 -- A descrambler/converter
- 9 -- Video monitor
- 11 -- Encryption processor
- 13 -- Terminal address module
- 15 -- Code key memory
- 17 -- Program memory
- 19 -- Signal path
- 20 -- Video presentation signal generator
- 21 -- Telephone
- 23 -- Telephone line
- 24 -- Check system of the central office
- 25 -- Telephone
- 27 -- Interface
- 29 -- Decryption system
- 30 30A or 30 N -- SMS
- 31 31A or 31 N -- PPV server
- 33 -- Table
- 35 -- Table

36 -- Processor  
37 -- Data receiver  
39 -- Charging device  
41 -- Input terminal  
43 -- Converter  
45 -- Switch  
46 -- Video output line  
47 -- Descrambler  
49 -- Microprocessor  
51 -- Bus  
53 -- Receiver by which remote control was carried out  
55 -- RAM  
56 -- Video presentation signal generator  
57 -- A/D converter  
59 -- Clock circuit  
61 -- Modem  
70A thru/or 70N -- Cable television operator control system  
72 -- Common network  
74 -- Microwave link.

---